ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMATICA Y ELECTRÓNICA

PROYECTO DE FORMACIÓN DE INGENIERÍA EN SISTEMAS INFORMÁTICOS

"ESTUDIO DE LAS TÉCNICAS DE CONTROL DE ACCESO A INTERNET Y SU APLICACIÓN EN LA RED DE DATOS DEL COLEGIO CORINA PARRAL DE LA CIUDAD DE CHIMBO".

TESIS DE GRADO

Previa la obtención del título de:

INGENIERA EN SISTEMAS

Presentado por:

REBECA DEL ROCÍO ANALUISA ZAPATA

RIOBAMBA – ECUADOR

2012

Dejo constancia de mi más sincero y profundo agradecimiento a la Escuela Superior Politécnica de Chimborazo, autoridades, docentes y gestores que hicieron posible el Proyecto de Profesionalización en Sistemas Informáticos, mismo que me ha brindado la oportunidad de continuar mis estudios profesionales.

Un reconocimiento especial al Ing. Alberto Arellano Director de este trabajo de investigación por su ayuda y colaboración para la culminación del mismo, de igual manera al Ing. Daniel Haro miembro del tribunal de tesis; a Directivos, maestros, personal administrativo y todas aquellas personas que contribuyeron con su sabiduría intelectual y paciencia para este logro.

A DIOS, POR SU
INFINITA BONDAD,
A MI MADRE, Y
FAMILIARES,
EN ESPECIAL
A MIS HIJOS: ANDRÉS,
VLADIMIR, SAMIR Y
DOMINICK,
MIS GRANDES TESOROS

NOMBRE	FIRMA	FECHA
Ing. Iván Menes **DECANO FIE**	.....	.....
Dr. Geovanny Vallejo **DIRECTOR PROFESIS**	.....	.....
Ing. Alberto Arellano **DIRECTOR DE TESIS**	.....	.....
Ing. Daniel Haro **MIEMBRO DEL TRIBUNAL**	.....	.....
Ing. Carlos Rodríguez **DIRECTOR DPTO DOCUMENTACIÓN**	.....	.....
NOTA DE LA TESIS	.....	

"Yo REBECA DEL ROCÍO ANALUISA ZAPATA, soy responsable de las ideas, doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO".

REBECA DEL ROCÍO ANALUISA ZAPATA

ÍNDICE DE ABREVIATURAS

ARP: Address Resolution Protocol, Protocolo de resolución de direcciones.

BSD: Software Distribution que traducido al español es llamado Distribución de software Berkeley.

ICMP: Internet Control Message Protocol. Protocolo Mensajes de Control de Internet

ISP: Internet Service Provider, Proveedor de servicios de internet.

IP: Internet Protocol o Protocolo de Internet

DHCP: Dynamic Host Configuration Protocol, que se traduce como Protocolo de configuración dinámica de servidores

DNS: acrónimo de Domain Name System, servidor de nombres de dominio.

FTP: File Transfer Protocol o Protocolo de Transferencia de Archivos

NAT: Network Address Translation, Traducción de Direcciones de Red

NIC: Network Information Center, Centro de Información sobre la Red.

NICs: Network Interface Cards, tarjetas de red

MAC: acrónimo de Media Access Control Address, que se traduce como dirección de Control de Acceso al Medio.

OSI: Open Systems Interconnection, Interconexión de Sistemas Abiertos.

PC: Computador u ordenador

RARP: Reverse Address Resolution Protocol,

RFC: Request For Comments, o Solicitud De Comentarios

SSH: Secure Shell

TCP: Transmission Control Protocol, Protocolo de Control de Transmisión

VPN: Virtual Private Network, o red virtual privada.

ÍNDICE GENERAL

CAPITULO III

ESTUDIO DE HERRAMIENTAS PARA EL CONTROL DE ACCESO A INTERNET

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

La Red en las empresas, centros educativos, instituciones financieras y otros permiten compartir recursos, o periféricos de elevado costo como impresoras, escáneres, trazadores gráficos, filmadoras, y otros, como los programas con el considerable ahorro de espacio en disco además su sencillez de actualización. Otra utilidad importante es como de medio de comunicación entre empleados, fuente de información, el correo electrónico es el servicio básico y otros más avanzados como la videoconferencia, o las aplicaciones que permiten compartir un documento entre varios usuarios, trabajando desde ordenadores distintos.

Gracias a los nuevos puntos de vista que han permitido que la sociedad evolucione, también aumenta la necesidad de buscar medidas que permitan controlar el acceso a parte de los servicios que ofrece Internet siendo importante que en los laboratorios de computación de los centros educativos se agiliten procesos informáticos, con nuevos y excelentes métodos para poder servir mejor a estudiantes, garantizando en todo momento que la búsqueda de información y el ingreso a sus contenidos este acorde al proceso de enseñanza aprendizaje en las diferentes áreas académicas, restringiendo el ingreso a información ofensiva que está en contra de los principios y normas reglamentarias que la rigen.

Ante lo anotado el presente trabajo de investigación se realizará para el laboratorio de computación que cuenta con servicio de internet gratuito donado por el gobierno central a instituciones educativas, pertenece al Colegio Nacional Mixto “Corina Parral”, está

ubicado en San José de Chimbo provincia Bolívar, es de una institución educativa con más de 40 años al servicio de la juventud estudiosa del cantón, tiene como misión la educar y elevar el nivel académico de cada uno de sus estudiantes para convertirlos en personas útiles a su familia y sociedad en general; y el objetivo principal es controlar el acceso a sitios indebidos por parte de los estudiantes de esta importante institución de la localidad.

Para su implementación se utilizará un sistema operativo confiable, versátil que facilite la administración de los servicios de manera segura, eficaz, y que su costo se mínimo, además su instalación y mantenimiento sea fácil de realizar.

En la estructura del trabajo investigativo se consideran los siguientes capítulos:

En el capítulo I, Marco referencial consta la descripción de las razones fundamentales para efectuar el estudio de las técnicas de control de acceso a internet y que objetivos nos permitirá alcanzar.

El capítulo II muestra una referencia teórica sobre los cortafuegos, características, ubicación, funcionamiento, tipos, implementación, configuración, inconvenientes, mantenimiento. También presenta información referente a los servidores proxy, características, ventajas, desventajas, configuración.

Un análisis comparativo de herramientas para servidores se muestra en el capítulo III, Squid, y Pfsense, características, requisitos hardware, software, funciones, instalación, configuración.

Finalmente en el capítulo IV al tener una herramienta seleccionada para el servidor se muestra los procesos necesarios para la implementación en el laboratorio de computación del plantel seguido de las conclusiones y recomendaciones que ha dejado proyecto.

Además será un aporte técnico práctico que servirá como referencia para el acceso y control de acceso en áreas similares en el plantel, y se lo podrá hacer de una manera eficaz porque la seguridad en el acceso a la información juega un papel importante dentro de la institución.

CAPITULO I

ESTUDIO DE LAS TÉCNICAS DEL CONTROL DE ACCESO A INTERNET Y SU APLICACIÓN EN LA RED DE DATOS EN EL COLEGIO "CORINA PARRAL" DE LA CIUDAD DE CHIMBO.

1.1 Antecedentes

En tan solo unos años las redes de computadores han pasado de ser algo esotérico sólo conocido y utilizado por unos pocos para llegar a ocupar un primer plano en cualquier medio informativo de carácter general.

La Red en las empresas, centros educativos, instituciones financieras y otros permiten compartir recursos, tales como periféricos de elevado costo: impresoras, escáneres, plotters, filmadoras, y otros, como los programas con el ahorro de espacio en disco y sencillez de actualización.

Otra utilidad importante es como de medio de comunicación entre empleados, fuente de información, el correo electrónico es el servicio básico y otros más avanzados como la videoconferencia, o las aplicaciones que permiten compartir un documento entre varios usuarios, trabajando desde ordenadores distintos.

La red puede conectarse al exterior, bien directamente o a través de un cortafuego o firewall, es decir una pasarela intermedia que permita controlar el acceso entrante y saliente para evitar problemas de seguridad. Cuando la red se conecta al exterior (normalmente Internet) aparecen nuevas aplicaciones que dan una mayor utilidad a las actividades realizadas, entre las que destacamos las actividades de marketing para promocionar y ofertar productos, y mostrar todos los servicios que ofrece la empresa o institución, logrando que los clientes obtengan información detallada de características, precios, o realicen sus pedidos a través de la red. También actividades relacionadas con la investigación, soporte técnico, educación, entretenimiento, soporte en línea, y mucho más.

El mundo virtual, o ciberespacio (nombre propuesto por W. Gibson en "Neuromancer", 1984) es un nuevo entorno social, construido a partir de las funcionalidades de Internet, donde podemos desarrollar muchas de las actividades propias del mundo real como informarnos, comunicarnos con la gente, estudiar, trabajar, divertirnos y otros. Entre sus características están:

- No hay distancias: todo está inmediatamente a nuestro alcance, no gastamos tiempo en desplazarnos.

- Tenemos a nuestro alcance casi toda la información del mundo; o por lo menos una parte significativa, plural y también de actualidad.

- Podemos comunicarnos con cualquier persona o entidad del mundo que "tenga presencia en el ciberespacio", para lo cual es necesario disponer por lo menos de e-mail. Son posibles comunicaciones en tiempo real o diferido (chat, e-mail.)

- Toda sensación y percepción está medida por aparatos: pantallas (para ver), altavoces (para oír), guantes de datos (para sentir tacto), etc.

- Podemos ofrecer una "nueva imagen" a los demás creando nuestra página web.

- Como es un entorno social, al igual que en el mundo real las personas debemos hacernos responsables de nuestras acciones.

- Sus infinitas posibilidades también generan nuevas problemáticas: para los padres resulta difícil controlar lo que hacen sus hijos en Internet, los profesores se encuentran tanto con alumnos que han construido muchos conocimientos erróneos como con alumnos que en algunos aspectos saben más que ellos.

Por la globalización a la que a diario nos estamos integrando, surge la necesidad de buscar medidas que permitan controlar el acceso a parte de los servicios que ofrece Internet los mismos que nos permiten día a día desenvolvernos en un área específica.

Cada vez son más los estudiantes que disponen de un ordenador y de conexión a Internet en su casa. Además, poco a poco los centros educativos van habilitando salas de estudio y puntos de acceso a Internet en laboratorios de computación, o en las bibliotecas para que los estudiantes, dentro del horario escolar o fuera de las horas de clase, puedan utilizar los computadores para trabajar y para buscar información en Internet. Con ello, las posibilidades de utilizar las TIC para "hacer deberes" cada vez están al alcance de más alumnos, y merece la pena aprovecharlo, ya que Internet está repleto de páginas de gran valor informativo, motivacional y también instructivo.

Las nuevas formas de investigación nos permiten romper barreras en el tiempo. Si se mira hacia atrás las actividades que debían desarrollarse se las cumplía en una gran cantidad de tiempo, mientras que en la actualidad con los avances tecnológicos y el uso de herramientas que permiten automatizar y simplificar procesos el ahorro de tiempo es notable beneficiando así a quienes a diario realizan diversas actividades.

Gracias a los nuevos puntos de vista que han permitido que la sociedad evolucione, surge la necesidad de que en los laboratorios de computación se agiliten procesos informáticos, con nuevos y excelentes métodos para poder servir mejor a quienes lo necesiten.

Estos antecedentes han despertado el interés en varios entornos, uno de ellos es el de las comunicaciones, debido a que en la actualidad se han desarrollado

varias tecnologías para facilitar el acceso de forma segura y confiable a la información que ofrece Internet en varios servidores remotos de las diferentes empresas.

El Laboratorio de Computación elegido para el estudio está ubicado en San José de Chimbo, Provincia Bolívar, es de una institución educativa con más de 40 años al servicio de la juventud estudiosa del cantón, tiene como misión la educar y elevar el nivel académico de cada uno de sus estudiantes para convertirlos en personas útiles a su familia y sociedad en general.

Cuenta con la infraestructura física para su funcionamiento, así: laboratorios de física, química, computación para guiar el proceso de enseñanza – aprendizaje, departamento de odontología, piscina, y áreas verdes para brindar servicio y recreación a sus estudiantes.

Para cada hora de practica en el laboratorio de computación asiste el profesor encargado de la asignatura y realiza el control respectivo, cuando requiere utilizar los servicios de Internet para investigación, clase práctica, u otra; establece la conexión mediante la cuenta y clave de usuario, mismas que no están disponible para los estudiantes; sin embargo al menor descuido o en horas extras a los estudiantes les resulta muy fácil acceder a páginas que ofrecen información indebida, además existen páginas que de forma automática bajan información y de forma inadvertida autocopian los programas virus, volviendo al equipo de trabajo inseguro.

Es por esta razón que en el Laboratorio de Computación de la Institución Educativa se desea incursionar en nuevos cambios que permitan acceder de una forma segura y confiable a los diferentes recursos que la institución brinda a sus estudiantes, y se requiere estudiar las diferentes técnicas de control para el acceso a Internet y su aplicación en la red de datos de la institución, para tener control sobre los usuarios que utilizan el laboratorio y acceden a Internet, restringiendo el acceso a páginas indebidas.

1.2 Justificación de la Tesis

Actualmente los estudiantes en las diferentes horas de práctica según la asignatura acceden a Internet para realizar consultas, descargar información, enviar o recibir correo electrónico, chatear, entre otros y no tienen ninguna dificultad para visitar sitios que ofrecen información ofensiva, no hay controles o seguridades en el acceso a los diferentes sitios de Internet, peor aún alguna medida para el tipo de información que ofrecen, la importancia de implementar técnicas de control de acceso a Internet está especialmente relacionada con la labor educativa que brinda el centro educativo, el equipo de computación del laboratorio con acceso a Internet lo ocupan estudiantes de toda la institución, así los alumnos de octavo de educación básica a tercero de bachillerato y además porque hay estudiantes que bajan información ofensiva y la dejan a fácil vista.

Además con la ampliación de cobertura del Servicio de Banda Ancha en la localidad y el aporte del Gobierno con este servicio para los centros educativos se cree necesario controlar más el acceso a Internet en el nuevo laboratorio de

computación, el mismo que dará oportunidad a más estudiantes para utilizar el servicio; también en las diferentes oficinas o departamentos se verá la necesidad de usar Internet.

Siendo estas algunas de las múltiples necesidades con las que cuenta el centro educativo, se ha creído conveniente realizar el estudio e investigación necesaria sobre las técnicas de control de acceso a Internet y luego de un análisis minucioso y comparación de la técnica más adecuada proceder a su implementación, brindando seguridad y protección a la información de cada equipo de trabajo, y porque con la fácil autocopia de programas virus lo vuelven inestable.

Se garantiza de esta manera que cuando los estudiantes de los diferentes cursos utilicen los computadores del laboratorio para sus horas de prácticas en las materias de computación y de especialidad no se encuentren con información desagradable, haya protección antivirus y tengan disponible los servicios de acuerdo a los privilegios respectivos.

Para poder crear este servicio se utilizará un sistema operativo confiable, versátil que facilite la administración de los servicios de manera segura, eficaz, y que su costo sea mínimo, además su instalación y mantenimiento sea fácil de realizar.

Este estudio permitirá iniciar un aporte técnico y práctico que servirá como referencia para el acceso y control de acceso en áreas similares en el plantel, se

lo puede hacer de una manera eficaz porque la seguridad en el acceso a la información juega un papel importante dentro de la institución.

1.3. Objetivos

1.3.1 Objetivo General

Estudiar las técnicas de control de acceso a Internet y su aplicación en la red de datos en el Colegio "Corina Parral" en la ciudad de Chimbo.

1.3.2. Objetivos Específicos

- Investigar las técnicas de control para el acceso a la información de Internet de manera confiable.
- Realizar el análisis comparativo de las técnicas estudiadas para su aplicación en la red de datos del colegio.
- Implementar las técnicas seleccionadas en la red de datos en el Colegio "Corina Parral" en la ciudad de Chimbo.

1.4. Hipótesis

El estudio de técnicas para el control de acceso a internet y su aplicación en la red de datos del Colegio "Corina Parral" mejorará el control de acceso de los usuarios a la información que brinda el Internet.

CAPITULO II

CORTAFUEGOS

2.1. QUE ES UN CORTAFUEGOS

Un Firewall o cortafuegos es un equipamiento, combinación de hardware y software que muchas empresas u organizaciones instalan entre sus redes internas e Internet, se utiliza para proteger la red interna (red local).

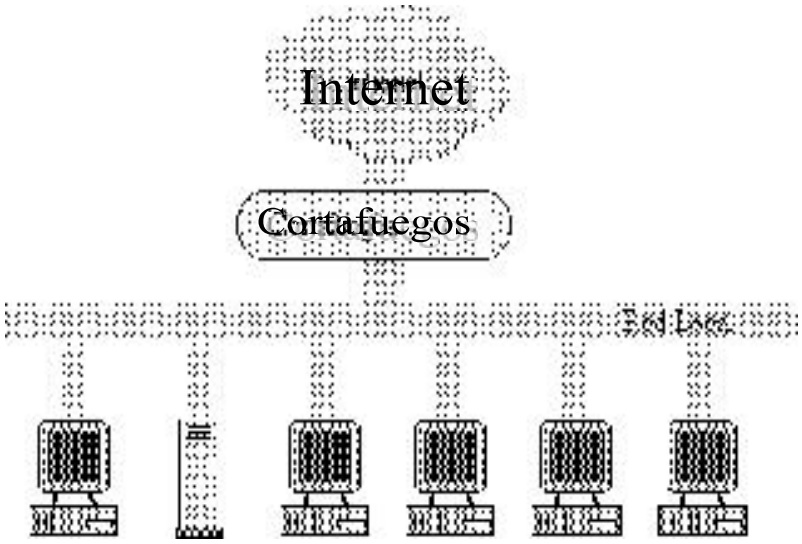


Figura II.1. Firewalls o Cortafuegos

Un cortafuego permite que sólo un tipo específico de mensajes pueda entrar y/o salir de la red interna. Esto protege a la red interna de los piratas o hackers que intentan entrar en redes internas a través del Internet.

Lo que hace el cortafuego es cortar o dejar pasar los intentos de comunicación que tiene todo el mundo (Internet) hacia nuestro ordenador o hacia nuestra red, según la situación del cortafuego, también puede controlar el tráfico generado desde nuestro ordenador o red hacia Internet.

El cortafuegos actúa basándose en normas que establece el administrador de seguridad, de red, o bien el usuario final. Estas reglas definen lo que tiene que hacer el cortafuego cuando encuentre un paquete que cumpla las características que nosotros le digamos. Aquí es donde se diferencian la mayoría de cortafuegos.

Un cortafuego, como cualquier dispositivo de red debe ser gestionado por alguien.

Un cortafuego es un programa o sistema que es capaz de leer la dirección y el remitente de todos los paquetes IP que intercambia un ordenador con la red. En base a una serie de reglas, el cortafuego permite o impide la entrada (conexiones remotas) o salida de información (Descubre back orifice o door). Las reglas se pueden cargar en la instalación o se pueden generar de forma interactiva e incremental, en base a las respuestas del usuario a las preguntas del cortafuego cada vez que detecta una entrada o salida nueva. Todo ello nos permite conocer el comportamiento de los programas que tenemos instalados.

Antes de hablar de lo que representan los cortafuegos en el ámbito de la seguridad en redes telemáticas convendría hablar un poco de qué se entiende por 'seguridad'. Puede haber múltiples definiciones de 'seguridad', se entenderá por seguridad en redes telemáticas a la protección frente a ataques e intrusiones en recursos corporativos por parte de intrusos a los que no se permite el acceso a dichos recursos. Por estos recursos entenderemos tanto el acceso a una carpeta compartida en servidor con NT, el acceso a los buzones de correo de los usuarios corporativos, o incluso el acceso a una sesión de Telnet de un servidor UNIX interno.

Evidentemente la forma de aislamiento más efectiva para cualquier política de seguridad consiste en el aislamiento físico, es decir, no tener conectada la máquina o la subred a otros equipos o a Internet (figura a).

Sin embargo, en la mayoría de organizaciones - especialmente en las de I+D - los usuarios necesitan compartir información con otras personas situadas en muchas ocasiones a miles de kilómetros de distancia, con lo que no es posible un aislamiento total. El punto opuesto consistiría en una conectividad completa con la red (figura b), lo que desde el punto de vista de la seguridad es muy problemático: cualquiera, desde cualquier parte del mundo, puede potencialmente tener acceso a nuestros recursos.

Un término medio entre ambas aproximaciones consiste en implementar cierta separación lógica mediante un cortafuegos (figura c).

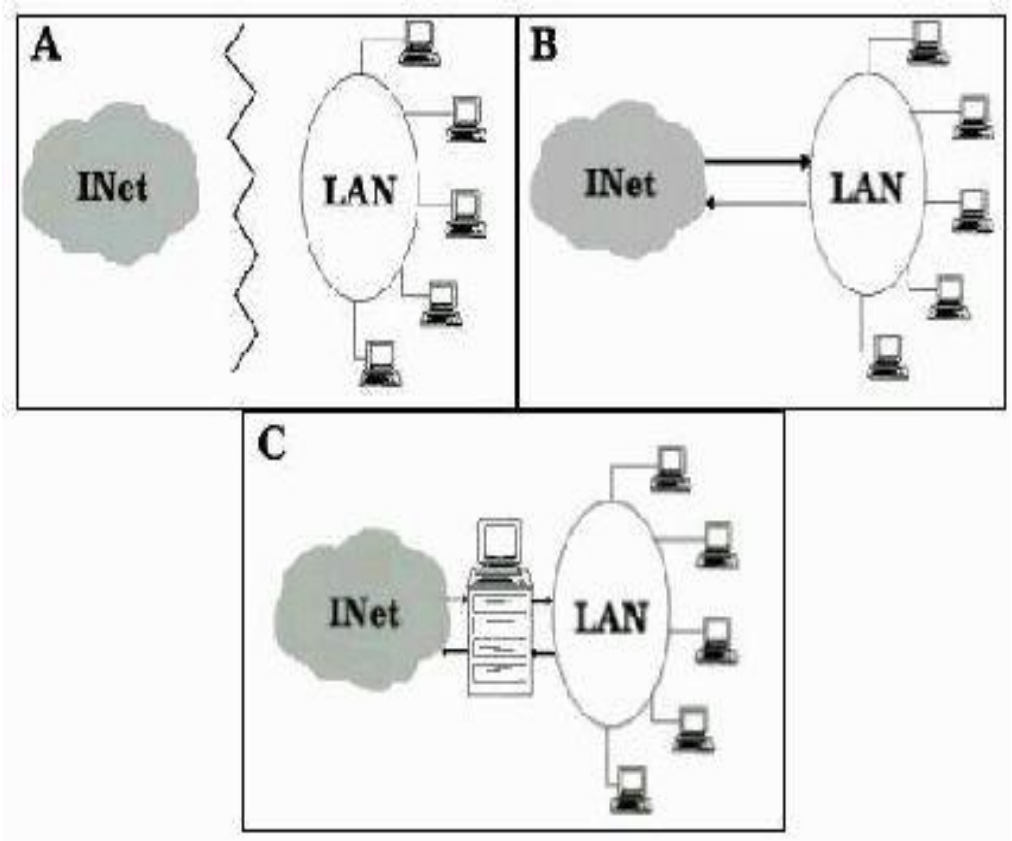


Figura II.2. Formas de aislamiento de computadores

La política de seguridad es (debería ser) un documento que está (debería estar) firmado por la alta gerencia de la empresa y mediante el cual se especifican distintos aspectos referentes a la seguridad informática de la empresa. Estos aspectos pueden ser desde cuantas letras han de tener las contraseñas de los usuarios corporativos y cada cuanto tiempo han de cambiarlas, qué protocolos (Telnet, http, smtp, ftp, etc.) van a permitir que hablen las máquinas internas con las externas y en su caso quien va a poder iniciar la conexión, y hasta la política que se va a seguir para permitir el acceso restringido a recursos internos.

Un cortafuegos nunca protegerá al cien por cien a estos recursos internos de acceso no autorizados ya que las técnicas de intrusión avanzan día a día (aunque el hardware y software de los cortafuegos también) y todos los días se descubren nuevos fallos (bugs) en sistemas operativos y software de servidores. Pero también es cierto que un firewall bien configurado junto con servidores bien configurados y protegidos puede poner las cosas muy difíciles a estos potenciales intrusos, por no decir imposibles (siempre teniendo en cuenta la política de seguridad de la empresa y a la correcta configuración de cortafuegos y servidores).

Los cortafuegos son uno de los dos enfoques básicos que se han dado al aspecto de la seguridad en redes telemáticas.

Estos dos enfoques han sido tradicionalmente la defensa en profundidad que se caracterizaba por proteger cada una de las máquinas susceptibles a ser accedidas por personas no autorizadas, y por otro lado la defensa perimetral consistente en llevar toda la carga correspondiente a la seguridad en la red corporativa al elemento de conexión de esta red corporativa con el exterior, o con las redes en las que potencialmente se encuentren las personas que puedan querer acceder a nuestros recursos de forma no autorizada, ya que está demostrado que un tanto por ciento elevado de los fraudes informáticos proceden del interior de las propias organizaciones.

Sus ventajas más notorias:

Protege de intrusiones.- Solamente entran a la red las personas autorizadas basadas en la política de la red en base a las configuraciones.

Optimización de acceso.- Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa si así se desea. Esto ayuda a reconfigurar rápida y fácilmente los parámetros de seguridad.

Protección de información privada.- Permite el acceso solamente a quien tenga privilegios a la información de cierta área o sector de la red.

Protección contra virus.- Evita que la red se vea infestada por nuevos virus que sean liberados.

La configuración correcta de cortafuegos se basa en conocimientos considerables de los protocolos de red y de la seguridad de la computadora. Errores pequeños pueden dejar a un cortafuego sin valor como herramienta de seguridad.

Los cortafuegos, por defecto, se activan siempre que se enciende el ordenador. Hay que configurarlo con cuidado, pues puede ocurrir que no funcione el correo electrónico o no se abran páginas Web en el navegador porque el 'firewall' no permite a estos programas acceder a Internet.

Para eso concentran todo el flujo entrante y saliente entre la computadora del usuario e Internet y bloquea los pedidos de enlaces no solicitados por los usuarios considerados

potencialmente inseguros, instalaciones clandestinas de programas y algunos hasta bloquean popups, publicidades, etc.

2.1.1. CORTAFUEGOS EN LAS EMPRESAS

Los Cortafuegos, se emplean tanto en grandes como en pequeñas redes para ofrecer seguridad frente a accesos no autorizados a la red interna, es simplemente un filtro que controla todas las comunicaciones que pasan de una red a otra, y en función de lo que sea, permite o deniega su paso. Para permitir o denegar una comunicación el cortafuego examina el tipo de servicio al que corresponde, como puede ser el web, el correo o el IRC. Dependiendo del servicio, el firewall decide si lo permite o no. Además, el cortafuegos examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

La función básica de un cortafuego ubicado en las empresas es ocultar el computador donde está instalado del resto de la red y protegerle de los accesos realizados desde otras redes. Hay que tener en cuenta que es, probablemente, la mejor medida de seguridad de un sistema y una de las que menos hay que actualizar.

El cortafuego formará una barrera para proteger a los ordenadores conectados a Internet en las dos direcciones: evitan una intrusión al computador desde la Red e impiden que los programas instalados accedan a Internet sin permiso.

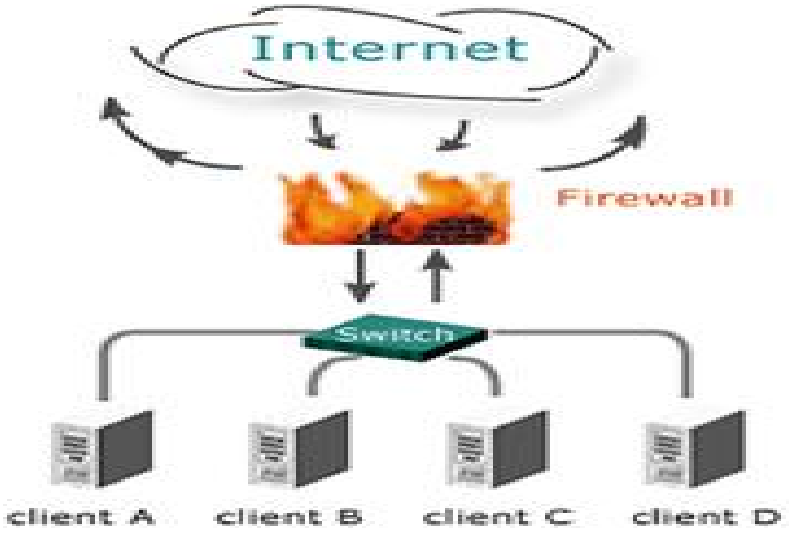


Figura II.3. Flujo de información entre clientes e internet

2.1.2. UN CORTAFUEGOS EN CASA

Un usuario particular raramente necesita un sistema de cortafuegos complejo, ya que el ordenador o el equipo de red puede tenerlo ya instalado. Si no es así, varias empresas ofrecen cortafuegos como solución de software para proteger el ordenador de una forma sencilla. La obtención de un software que podrá adquirir por un precio bajo entre los 50 y los 100 dólares suele ser suficiente para proteger la mayoría de los ordenadores particulares.

Los cortafuegos han sido creados para evitar el acceso no autorizado a un sistema o a una red. Al igual que la puerta cerrada de una casa, el cortafuegos bloquea a todos los intrusos menos a los que creamos conveniente. Es un programa de software que se instala en un ordenador o en una red, o bien una solución formada por hardware y software.

Aunque el usuario medio pueda creer que eso de los ataques no es algo que le pueda suceder en su casa a su computadora, los cortafuegos se convierten en un elemento imprescindible si se utiliza mucho el ordenador y se está conectado permanentemente mediante ADSL o cable. El firewall evitará la entrada de los programas que rastrean direcciones IP (un número que se asigna cada ordenador conectado) a la caza de conexiones por banda ancha que parasitar, a la vez que frustrará los intentos de los programas espía de robar datos del PC y de los troyanos de abrir brechas de seguridad.

En Internet se pueden encontrar versiones no profesionales de cortafuegos, suficientes para el usuario doméstico, que se pueden descargar de forma gratuita. El más popular es ZoneAlarm, aunque existen otros como Outpost, Kerio o Sygate.

También hay cortafuegos integrados en los programas antivirus o en el propio sistema operativo. El que viene con Windows XP no es demasiado seguro porque, al contrario que otros cortafuegos, sólo vigila las conexiones entrantes, mientras que el tráfico de salida no está restringido.

Al momento de instalar considerar:

Cortafuegos basados en host—software: que protege exclusivamente el ordenador en él que está instalado.

Cortafuegos basados en red—instalados entre el módem del ADSL o del cable y su red doméstica: para proteger todos los ordenadores conectados, es una máquina o dispositivo que controla el tráfico entre la red interna y externa de una organización.

Cuando se instala un cortafuego en el sistema, todos los datos enviados al sistema y que parten de éste se supervisan y se comparan con un conjunto de criterios de seguridad definidos por el usuario. Todos los datos que no cumplan con estos criterios se bloquean.

El basado en hardware suele ser mucho más fiable y menos sujeto a ataques y problemas, también cuesta mucho más dinero que el que utiliza software (hay programas gratuitos que realizan esta función de control).

Ejemplo el Norton Personal Firewall de Symantec protege su privacidad al evitar que la información confidencial se envíe fuera sin su consentimiento. Empresas en línea disponen además de un comprobador de seguridad en línea que puede utilizar para saber el grado de exposición a las amenazas de Internet e identificar el tipo de seguridad que necesita.

Bajo Windows, si el sistema operativo que ejecuta en el ordenador es Windows XP ya tendrá un cortafuegos que viene incluido.

En Macintosn**,** si dispone de un Macintosh o de una versión diferente de Windows, compruebe si tiene instalado un cortafuegos. Para ello, busque si hay programas cortafuegos o firewall en la carpeta Archivos de programa de Windows o en la carpeta Aplicaciones del Mac. Si no lo tiene instale el de otra marca como el de comercial. Compruébelo también en los manuales de los dispositivos de su red doméstica para saber si incluyen firewall de hardware integrado.

2.1.3. PROTECCIÓN AVANZADA

Si lleva un negocio desde su casa y dispone de información que no puede permitirse el lujo de perder, debería considerar la posibilidad de invertir en algo más avanzado. Por ejemplo, un contable que tiene su información personal y la del cliente almacenado en el ordenador, puede pensar que merece la pena invertir en un cortafuego y de un servicio que se lo gestione.

Algunas funciones de productos en varios sistemas operativos requieren hardware avanzado o adicional.

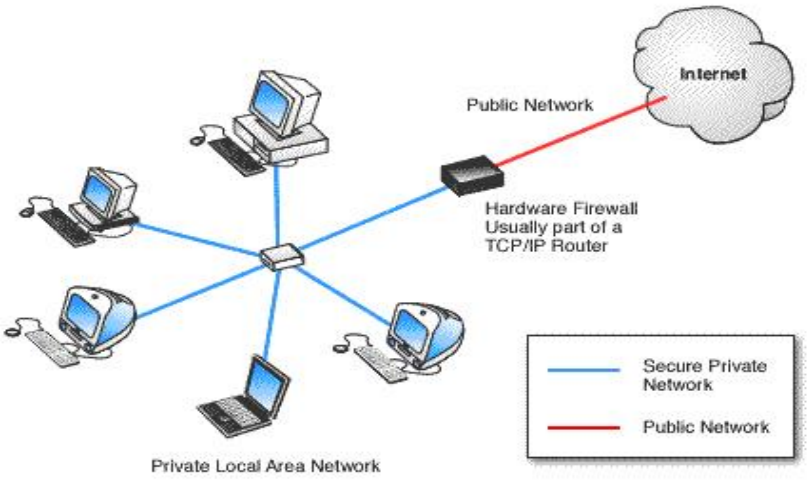


Figura II.4. Protección avanzada

2.1.4. ASIGNACIÓN DE PUERTOS

El puerto es un canal de comunicación para computadores en una red, es una numeración lógica que se asigna a las conexiones, tanto en el origen como en el destino. No tiene ninguna significación física.

El permitir o denegar acceso a los puertos es importante porque las aplicaciones servidoras (que aceptan conexiones originadas en otro ordenador) deben 'escuchar' en un puerto conocido de antemano para que un cliente (que inicia la conexión) pueda conectarse.

Esto quiere decir que cuando el sistema operativo recibe una petición a ese puerto, la pasa a la aplicación que escucha en él, si hay alguna, y a ninguna otra. Los servicios más habituales tienen asignados los llamados puertos bien conocidos, por ejemplo el 80 para web, el 21 para ftp, el 23 para telnet, etc. Así, cuando usted solicita una página web, su navegador realiza una conexión al puerto 80 del servidor web, y si este número de puerto no se supiera de antemano o estuviera bloqueado no podría recibir la página.

Por convención, hay una correspondencia entre un cierto número de puerto y el servicio que lo utiliza para servidores, 80 para servidores web, 21 para servidores FTP.

2.1.5. ESTADOS DE UN PUERTO

Un puerto puede estar:

Abierto: Acepta conexiones. Hay una aplicación escuchando en este puerto. Esto no quiere decir que se tenga acceso a la aplicación, sólo que hay posibilidad de conectarse.

Cerrado: Se rechaza la conexión. Probablemente no hay aplicación escuchando en este puerto, o no se permite el acceso por alguna razón. Este es el comportamiento normal del sistema operativo.

Bloqueado o Sigiloso: No hay respuesta. Este es el estado ideal para un cliente en Internet, de esta forma ni siquiera se sabe si el ordenador está conectado. Normalmente este comportamiento se debe a un cortafuego de algún tipo, o que el ordenador está apagado.

2.1.6. CÓMO FUNCIONAN LOS FIREWALL

Se manejan por zonas (seguras o no) o bien por niveles de seguridad, los que establece el usuario según el grado de permisividad que le imponga al equipo. Pero luego el programa se va configurando con el tiempo. Como decimos en cada review (revisión), en realidad con los Firewalls no hay que hacer nada, sólo configurarlos según las necesidades o gustos del usuario, cosa que no termina con la instalación.

Luego de la instalar el firewall, una vez que el usuario se conecta a Internet (o aún antes) comienza a trabajar el programa. Los primeros días de uso pueden ser un tanto engorrosos ya que tanto el usuario como el programa "aprenden" mutuamente. El usuario aprende las funciones y el programa qué cosas debe dejar pasar, qué bloquear y qué programas dejar conectar, por eso al principio son puras preguntas, hasta que se van conformando las reglas de uso en la medida que el usuario haga determinadas acciones con las alarmas que pueden ser de varios tipos. Con este tipo de aviso el programa pide que se defina la regla que se va a aplicar entre alguna de las posibles.

Una vez que se determina qué hacer con esa acción (por ejemplo permitir que un

programa se conecte siempre a Internet), con cada cartel de alerta se van configurando las reglas ya que luego ese aviso no va a volver a aparecer. Con el tiempo estos avisos se reducen al mínimo.

Por cada acción crean un registro de la actividad (log) para el posterior análisis del usuario.

2.1.7. TIPOS DE PELIGROS QUE PUEDE EVITAR UN FIREWALL

- Instalación y ejecución de programas instalados clandestinamente desde Internet, por ejemplo vía aplicaciones **ActiveX** o Java que pueden llegar a transferir datos personales del usuario a sitios.

- Acceso de terceros por fallas o errores de configuración de Windows (por ejemplo de NetBIOS).

- Instalación de publicidad (advertisers) o elementos de seguimiento (track) como las cookies.

- Troyanos: aplicaciones ocultas que se descargan de la red y que pueden ser usadas por terceros para extraer datos personales. A diferencia del virus, estos troyanos son activados en forma remota por un tercero.

- Reducción del ancho de banda disponible por el tráfico de banners, popus, sitios no solicitados, y otro tipo de datos innecesarios que vuelven lenta la conexión.

- Utilización de la línea telefónica por terceros por medio de **Dialers** (programas que cortan la actual conexión y utilizan la línea para llamadas de larga distancia)

2.1.8. ¿POR QUÉ SON TAN POPULARES LOS CORTAFUEGOS (FIREWALLS)?

Es posible que haya oído alguna vez la expresión "no pudo hacer esto porque no me lo permite el cortafuegos.

Si dispone en su casa u oficina de una conexión rápida a Internet (ADSL, Cable, RDSI, u otra) es posible que esta, además sea permanente, es decir, que aunque no lo utilice, o incluso aunque esté su computador apagado, permanece conectado a Internet a través del modem o router. Esa conexión permanente hace que su ordenador o red de ordenadores sea una víctima fácil de cualquier persona con interés en destruir, copiar o manipular información de su equipo.

Otra de las razones que ha extendido la popularidad de los cortafuegos es el poder limitar a que servicios y lugares de Internet se desea que puedan conectarse los usuarios de una red. Por ejemplo, evitar que en una oficina se colapse la conexión a Internet y baje la productividad porque los empleados se descargan música o ven vídeos.

2.1.9. UBICACIÓN DE LOS CORTAFUEGOS (FIREWALLS)

Un Firewall (Cortafuegos) es sencillamente un dispositivo que se coloca antes del router o modem y que filtra los contenidos que entran y salen del exterior. Una persona autorizada puede definir normas para esos filtros, de forma que cada vez que los filtros detecten una circunstancia eviten la conexión.

Los filtros de salida que podemos poner en le cortafuegos son del tipo:

- Que personas no acceden a Internet
- Que usuarios y empleados no puedan acceder a servicios de bajarse música
- Quienes de un departamento u oficina específica no pueden ir a un sitio Web.

Los filtros de entrada que podemos poner en el cortafuegos son del tipo:

- Que desde el exterior nadie pueda acceder a los ordenadores de nuestra red, menos al servidor X (por ejemplo el servidor de correo o Web)
- Que desde el exterior sólo un usuario autorizado pueda entrar en nuestra red.

2.1.10. MÉTODOS DE FILTRADO E INSPECCIÓN

Los cortafuegos utilizan tres o más sistemas de controlar el tráfico, estos son:

- **Filtrado de paquetes**

Cada paquete de información que entra o sale de la red es analizado y si contradice una de las normativas impuestas, se descarta. Una normativa podría ser prohibir el acceso a una Web determinada con IP de por ejemplo A.B.C.D, si el cortafuego direcciona el paquete IP y ve que va destinado a A.B.C.D lo bloquea y al usuario le aparece que la conexión no es posible.

- **Servicio Proxy**

No se inspeccionan paquetes sino contenidos, es decir, un usuario quiere conectar con la Web www.34t.com, el cortafuego baja la página completa, la analiza, y si no contradice las normas, la envía al usuario.

- **Inspección "Stateful"**

Es el método más actual de inspección. Consiste en una inspección lógica que, añadida al filtrado de paquetes da un alto nivel de protección. El "Stateful Inspection" analiza cada paquete de salida (solicitud) a Internet, y analiza los paquetes de respuesta. Si ambos no mantienen una coherencia, los descarta. Es decir, descarta automáticamente todo aquello que no es razonable en un contexto determinado a fin de evitar ataques desde el exterior

2.2. TIPOS DE CORTAFUEGOS SEGÚN EL NIVEL OSI

Existen muchos tipos de cortafuegos, no obstante la clasificación más clara quizás sería la que los diferencia según la forma de implementar la política de seguridad de la empresa atendiendo al nivel de la capa OSI en la que se implementa dicha política de seguridad.

- En un primer lugar existen los cortafuegos de nivel 3 de la capa OSI, esto es, de nivel de red o lo que es lo mismo, nivel IP en redes TCP/IP como Internet. Estos cortafuegos pueden ser considerados como filtros de paquetes ya que lo que realizan a fin de cuentas es un filtrado de los intentos de conexión atendiendo a direcciones IP origen y destino y puerto de destino de los paquetes IP. Esto quiere decir que en la política de seguridad de la empresa podremos indicar que sólo dejaremos pasar paquetes destinados al puerto 25 (puerto de SMTP para correo electrónico) de nuestro servidor corporativo. También podremos especificar desde qué direcciones IP origen dejaremos acceso a nuestros servidores públicos. Este tipo de cortafuegos vienen implementados en la mayoría de routers comerciales.

- Otra posibilidad de implementación de cortafuegos es a nivel 4 de OSI, esto es a nivel de transporte o de TCP en redes TCP/IP. En este nivel ya se puede atender aspectos de sí los paquetes son de inicio de conexión o se corresponden con paquetes cuyas conexiones están ya establecidas.

A grandes rasgos los cortafuegos a nivel de circuitos ya tratan con números de secuencias de paquetes TCP/IP. Si los paquetes pertenecen a una conexión o si no se corresponden con ninguna conexión establecida.

- Por último nos quedan los cortafuegos a nivel 7 de la capa OSI, esto es, a nivel de aplicación. Estos cortafuegos actúan a modo de proxy para las distintas aplicaciones que van a controlar. Por lo pronto ya se ve que con estos cortafuegos no será posible dejar pasar todos los protocolos (al menos de manera segura, esto es, no es frecuente ver cortafuegos a este nivel), pero lo que sí es cierto es que podremos llegar al detalle en cuanto a la posibilidad de implementar políticas de seguridad para estos protocolos.

La implantación de cortafuegos de distintos niveles de aplicación no tiene que ser excluyentes sino complementarias.

2.2.1. IMPLEMENTACIONES DE TIPOS DE CORTAFUEGOS

Existen varias implementaciones de cortafuegos que pueden ser organizadas de las formas siguientes:

2.2.2. CORTAFUEGOS DE FILTRADO DE PAQUETES

Utilizan routers con reglas de filtrado de paquetes para conceder ó denegar acceso en base a la dirección fuente, dirección destino y puerto. Ofrecen seguridad mínima pero a

muy bajo costo y puede ser una alternativa apropiada para entornos de bajo riesgo. Son rápidos, flexibles y transparentes. Las reglas de filtrado no suelen ser fácilmente mantenidas en un router, pero existen herramientas disponibles para simplificar las tareas de crear y mantener las reglas.

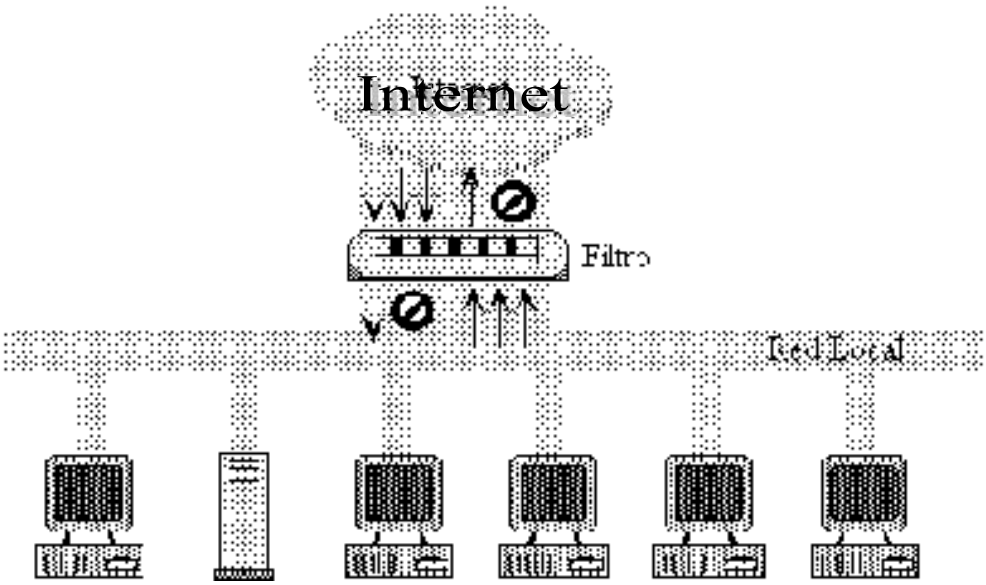


Figura II.5. Cortafuegos de filtrado de paquetes

El Enrutador de protección para hacer el filtrado de paquetes: Enruta o bloquea paquetes según lo determina la política de seguridad del sitio.

Los riesgos de los cortafuegos basados en el filtrado de paquetes son:

1) Las direcciones origen y destino y los puertos contenidos en la cabecera del paquete IP son la única información disponible para que el router tome la decisión de si permite o no acceso de tráfico a una red interna.

2) No protegen contra "spoofing" (ó engaño) de direcciones DNS ó IP.

3) Un atacante tendrá un acceso directo a cualquier computador de la red interna una vez que el acceso haya sido concedido por el cortafuego.

4) En algunos cortafuegos de filtrado de paquetes no se soporta la autentificación fuerte de usuarios.

5) Proporcionan poca ó nula información útil de "logging" (de registro).

2.2.3. CORTAFUEGOS DEL NIVEL DE APLICACIÓN

Utilizan programas servidor (denominados "proxies") que se ejecutan en el cortafuegos. Estos "proxies" toman las peticiones externas, las examinan y reenvían peticiones legítimas al computador interno que proporciona el servicio apropiado. Los cortafuegos del nivel de aplicación pueden soportar funciones como por ejemplo la autentificación de usuario y el registro.

Debido a que un cortafuego del nivel de aplicación se considera como el tipo más seguro de cortafuegos, esta configuración proporciona un conjunto de ventajas a la organización de riesgo medio-alta:

1) El firewall o cortafuegos puede configurarse como la única dirección de computador que es visible para la red externa, requiriendo que todas las conexiones hacia ó desde la red interna se realicen a través del firewall.

2) La utilización de "proxies" para diferentes servicios impide el acceso directo a servicios de la red interna, protegiendo a la organización contra computadores internos mal configurados ó no seguros.

3) La autentificación fuerte de usuario puede ser obligada por los cortafuegos del nivel de aplicación.

4) Los "proxies" pueden proporcionar registro (ó "logging") detallado en el nivel de aplicación. Los cortafuegos del nivel de aplicación deberían configurarse de modo que el tráfico de red externo (fuera del perímetro de seguridad) aparezca como si el tráfico lo originó el cortafuegos (es decir, sólo el cortafuegos está visible para las redes externas). De esta forma, no está permitido el acceso directo a los servicios de red de la red interna. Todas las peticiones entrantes para los diferentes servicios de red como telnet, ftp, http, rlogin, etc., sin tener en cuenta qué computador de la red interna es el destino final, deben ir a través del "proxy" apropiado del cortafuego.

Los cortafuegos del nivel de aplicación requieren que se soporte un "proxy" para cada servicio, por ejemplo ftp, http, etc. Cuando un servicio se requiere que no esté soportado por un "proxy", la organización posee tres alternativas:

1) Denegar el servicio hasta que el fabricante del cortafuego desarrolle un "proxy seguro". Esta es la alternativa preferida cuando los nuevos servicios Internet introducidos poseen vulnerabilidades no aceptables.

2) Desarrollar un "proxy a medida". Esta opción es una tarea bastante difícil y sólo debería emprenderse por organizaciones técnicas sofisticadas.
3) Pasar el servicio a través del cortafuego. Utilizando lo que se denomina normalmente "plugs", la mayoría de cortafuegos del nivel de aplicación permiten que los servicios se pasen directamente a través del cortafuego con sólo un mínimo de filtrado de paquetes. Esto puede limitar algunas de las vulnerabilidades pero puede comprometer la seguridad de los sistemas detrás del cortafuego.

Cuando un servicio Internet interno (dentro de la frontera de seguridad) no está soportado por un "proxy" se requiere pasar a través del cortafuego, el administrador del cortafuego debe definir la configuración ó "plug" que permita el servicio pedido. Cuando está disponible un "proxy" del fabricante del cortafuego, el "plug" se inhabilitará y el "proxy" se hará operativo. Todos los servicios Internet internos (de dentro del perímetro de seguridad) deben ser procesados por software "proxy" del cortafuego. Si se pide un nuevo servicio, este no se estará disponible hasta que se disponga de un "proxy" del fabricante del cortafuego y sea verificado por el administrador del cortafuego. Se puede desarrollar un "proxy a medida" por la propia organización ó por otros fabricantes y sólo se podrá utilizar cuando sea aprobado por el responsable de seguridad de información.

2.2.4. CORTAFUEGOS HÍBRIDOS

Combinan los tipos de cortafuegos anteriores y los implementan en serie en vez de en paralelo.

Si se conectan en serie, se mejora la seguridad total. Si se conectan en paralelo, entonces el perímetro de seguridad de red sólo será tan seguro como el menos seguro de los métodos utilizados. En entornos de medio a elevado riesgo un cortafuego híbrido puede ser la elección ideal de cortafuegos.

2.2.5. OTROS CORTAFUEGOS

2.2.5.1. CORTAFUEGOS PARA INTRANETS

Aunque los cortafuegos normalmente se colocan entre una red corporativa y la red no segura del exterior (ó Internet), en grandes organizaciones, los cortafuegos se utilizan a menudo para crear subredes diferentes dentro de la red interna (denominada también Intranet). Los "cortafuegos para Intranets" se utilizan para aislar una subred particular de la red corporativa total. La razón del aislamiento de un segmento de red puede ser que ciertos empleados sólo pueden acceder a subredes guardadas por estos cortafuegos sólo en base a una necesidad concreta. Un ejemplo puede ser un cortafuego para el departamento de nóminas ó contabilidad de una organización.

La decisión de utilizar un cortafuego Intranet se basa generalmente en la necesidad de hacer cierta información disponible para algunos pero no para todos los usuarios internos ó para proporcionar un alto grado de responsabilidad para el acceso y utilización de información sensible ó confidencial. Para cualquier sistema que guarde aplicaciones críticas de la organización ó que proporcione acceso a información sensible ó confidencial, deberían utilizarse cortafuegos internos ó routers de filtrado de paquetes

para proporcionar control de acceso fuerte y soportar auditoría y registro. Estos controles deberían utilizarse para dividir la red corporativa interna a la hora de soportar políticas de acceso desarrolladas por los propietarios de información designados.

2.2.5.2. CORTAFUEGOS CON CAPACIDAD VPN

Las redes privadas virtuales ó VPN (Virtual Private Networks) permiten a las redes seguras comunicarse con otras redes seguras utilizando redes no seguras como Internet. Puesto que algunos cortafuegos proporcionan la "capacidad VPN", es necesario definir una política de seguridad para establecer VPNs. Cualquier conexión entre cortafuegos sobre redes públicas utilizan VPNs cifradas para asegurar la privacidad e integridad de los datos que se pasan a través de la red pública. Todas las conexiones VPN deben ser aprobadas y gestionadas por el administrador de servicios de red. Deben establecerse los medios apropiados para distribuir y mantener claves de cifrado antes del uso operacional de los VPNs.

2.2.6. CORRESPONDENCIA ENTRE TIPO DE CORTAFUEGOS Y NIVEL DE RIESGO DE SEGURIDAD

2.2.6.1. CORTAFUEGOS DE FILTRADO DE PAQUETES

Para Entornos de Alto Riesgo (por ejemplo hospitales) "no es aceptable".

Para Entornos de Riesgo Medio (por ejemplo, Universidades) "mínima seguridad".

Para Entornos de Bajo Riesgo (por ejemplo, pastelería) "elección recomendable".

2.2.6.2. CORTAFUEGOS DEL NIVEL DE APLICACIÓN

Para Entornos de Alto Riesgo, "opción efectiva".

Para Entornos de Riesgo Medio, "elección recomendada".

Para Entornos de Bajo Riesgo, "elección aceptable".

2.2.6.3. CORTAFUEGOS HÍBRIDOS

Para Entornos de Alto Riesgo, "elección recomendada".

Para Entornos de Riesgo Medio, "opción efectiva".

Para Entornos de Bajo Riesgo, "elección aceptable".

2.2.7. ARQUITECTURAS DE CORTAFUEGOS

Los cortafuegos se pueden configurar en diferentes arquitecturas, proporcionando diversos niveles de seguridad a diferentes costos de instalación y operación. Las organizaciones deberían hacer corresponder su perfil de riesgo con el tipo de arquitectura de cortafuegos seleccionada. Las principales arquitecturas de cortafuegos son:

2.2.7.1. COMPUTADOR MÚLTI-PUERTO (Ó "MULTI-HOMED HOST")

Se trata de un computador que tiene más de un interface de red, cada interface se conecta a segmentos de red física y lógicamente separados. Un computador de doble

puerto (un computador con dos interfaces) es el ejemplo más común de computador multi-puerto. Un cortafuego de doble puerto es un cortafuego con dos tarjetas de red (ó NICs, Network Interface Cards), cada interface conectado a una red diferente. Por ejemplo, una interface de red normalmente se conecta a la red externa no segura, mientras que el otro se conecta a la red interna ó segura.

En esta configuración, uno de los principios de seguridad clave es no permitir que el tráfico procedente de la red no segura se encamine directamente a la red segura, el cortafuegos siempre debe actuar como intermediario. El encaminamiento del cortafuego se inhabilitará para un cortafuegos de doble puerto para que los paquetes IP de una red no se encaminen directamente de una red a la otra.

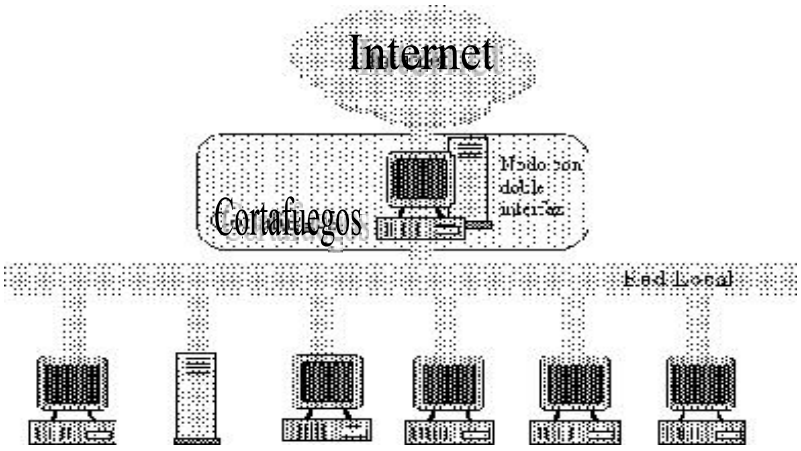


Figura II.6. Cortafuego con computador multi-puerto

2.2.7.2. COMPUTADOR PANTALLA (Ó "SCREENED HOST")

Un cortafuego con esta arquitectura utiliza un computador denominado "bastión" para que todos los computadores de fuera se conecten, en vez de permitir conexión directa a

otros computadores internos menos seguros. Para realizar esto, un router de filtrado de paquetes se configura para que todas las conexiones a la red interna desde la red externa se dirijan hacia el computador "bastión".Si se debe utilizar un cortafuegos de filtrado de paquetes, entonces un computador "bastión" debería establecerse para que todas las conexiones desde la red externa vayan a través del computador "bastión" para impedir que la conexión Internet directa entre la red de la organización y el mundo exterior.

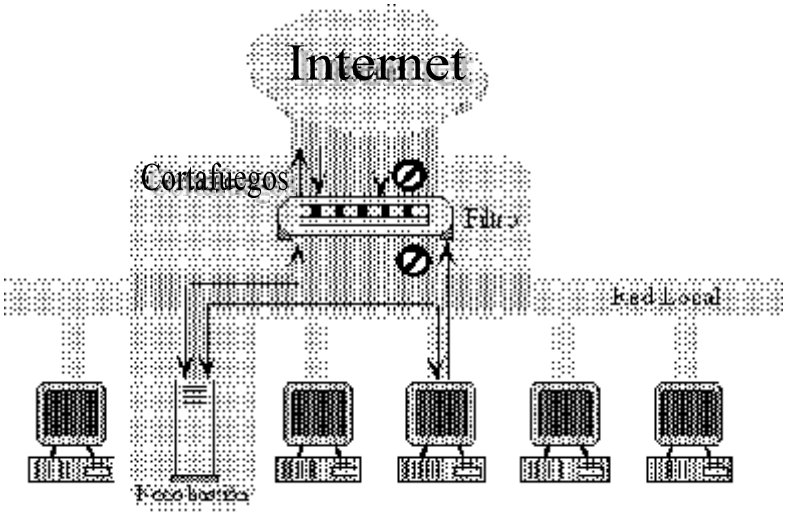


Figura II.7. Cortafuego con computador pantalla

2.2.7.3. SUBRED PANTALLA (Ó "SCREENED SUBNET")

Esta arquitectura es esencialmente similar a la arquitectura del "computador pantalla", pero añade una capa extra de seguridad creando una red en la que reside el computador "bastión" (denominada "red perimetral") que se encuentra separada de la red interna. Una "subred pantalla" se crea añadiendo una red perimetral que separe la red interna de la externa. Esto asegura que si existe un ataque con éxito en el computador bastión, el

atacante está restringido a la red perimetral por el "router pantalla" que se conecta entre la red interna y la red perimetral.

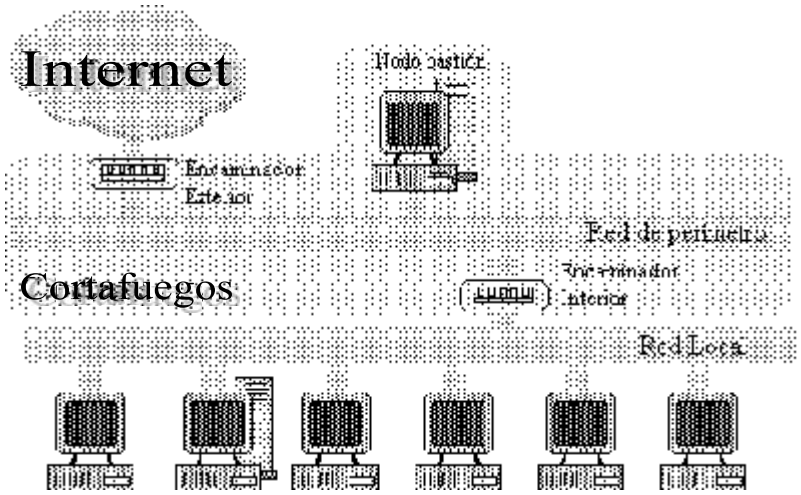


Figura II.8. Cortafuego con subred pantalla

2.2.8. QUE PUEDE Y QUE NO PUEDE HACER UN CORTAFUEGOS:

2.2.8.1. QUE PUEDE HACER UN CORTAFUEGO

Los cortafuegos pueden hacer mucho por la seguridad de un sitio. De hecho, algunas de sus ventajas se extienden más allá de la seguridad, como describimos a continuación.

Un cortafuego es una fuente de decisiones de seguridad

Un cortafuego es como un cuello de botella. Todo el tráfico que entra y sale debe pasar por este estrecho punto de inspección. Un cortafuego da un grado de eficiencia enorme

a la seguridad de redes porque permite concentrar sus medidas de seguridad en este punto de inspección: el punto donde su red se conecta con internet.

Resulta más eficiente centrar su seguridad de esta forma que extender sus decisiones de seguridad por todas partes, intentando cubrir todas las bases de manera individual.

Un cortafuego puede reforzar las políticas de seguridad

Muchos de los servicios que las personas demandan de internet son, por su propia naturaleza, inseguros. Un cortafuego es como el agente de tránsito para estos servicios. Refuerza las políticas de seguridad del sitio, permitiendo que pasen solo los servicios aprobados y aquellos que cumplen las reglas establecidas para ello.

Un cortafuego puede almacenar su relación con internet de manera eficiente

Debido a que todo transita por el cortafuego, éste proporciona un buen lugar para reunir información sobre el uso, o mal uso, de sistemas y redes. Con un punto único de acceso un cortafuego puede registrar lo que ocurre entre la red protegida y la red externa.

Un cortafuego limita la exposición

Un cortafuego se utiliza para mantener separada una sección de su red de otra. Esto evita que los problemas que impactan una sección de la red se extiendan a través de

toda ella. Unas veces porque una sección de la red puede ser más confiable que otra, y otras debido a que una sección es más sensible que otra.

2.2.8.2. QUE NO PUEDE HACER UN CORTAFUEGO

Los cortafuegos ofrecen excelente protección contra las amenazas a la red, pero no son una solución de seguridad total. Ciertas amenazas están fuera del control del cortafuego. Debe encontrar otras formas de protegerse contra ellas incorporando seguridad física, seguridad para anfitrión y educación para el usuario en su plan general de seguridad.

Un cortafuego no puede proteger la red contra personas internas

Un cortafuegos puede evitar que un usuario del sistema envíe información del propietario fuera de la organización a través de su conexión de red, esto también se evitaría no teniendo ninguna conexión con la red externa. Pero ese mismo usuario podría copiar los datos en disco o papel y sacarlos del edificio.

Los usuarios internos pueden robar datos, dañar el hardware y el software y modificar los programas sin acercarse al cortafuego. Las amenazas desde dentro requieren medidas de seguridad internas.

Un cortafuego no puede protegerlo contra conexiones que no pasan por él

Un cortafuegos puede controlar el tránsito que pasa por él de manera eficaz; Sin embargo, no hay nada que pueda hacer con el tránsito que no pasa por él. No puede

proteger la red con los accesos telefónicos conmutados si éstos están detrás del cortafuego.

Un cortafuego no puede proteger contra amenazas antes desconocidas

Un cortafuego está diseñado para proteger contra amenazas conocidas. Uno bien diseñado puede proteger también contra nuevas amenazas (al negar todos menos los servicios confiables, un cortafuegos evita que las personas instalen servicios nuevos e inseguros). Sin embargo ningún cortafuego puede defenderse de manera automática contra cada amenaza nueva que surge. No puede instalar un cortafuego una sola vez y esperar que lo proteja para siempre, hay que mantenerlo y actualizarlo.

Un cortafuego no puede proteger contra virus

Los cortafuegos no pueden mantener los virus de computadores y Macintosh fuera de la red. Aunque muchos cortafuegos revisan todo el tránsito que entra para determinar si puede pasar a la red interna, la exploración ocurre en su mayoría a nivel de direcciones fuente y destino y números de puerto, no en los detalles de los datos. Aun cuando se tenga filtrado de paquetes o software proxy complejo, la protección contra virus en un cortafuego no es muy práctica. Hay demasiados tipos de virus e infinidad de formas en que uno de ellos puede ocultarse dentro de los datos.

Detectar un virus al azar en un paquete de datos que pasa a través de un cortafuego es muy difícil; requiere de:

- Reconocer que el paquete es parte de un programa.
- Determinar cómo debe verse el programa.
- Determinar que el cambio se debe a un virus.

2.2.9. IDENTIFICACION Y CLASIFICACION DE AMENAZAS A LOS CORTAFUEGOS DE FILTRADO DE PAQUETES DE NIVEL RED/TRANSPORTE. CONDICIONES DE UTILIZACION SEGURA.

El propósito de un cortafuegos de filtrado de paquetes es proporcionar un punto de defensa y acceso controlado y auditado para servicios, tanto desde dentro como desde fuera de una red privada de una organización, permitiendo y/o denegando el flujo de paquetes a través del cortafuegos.

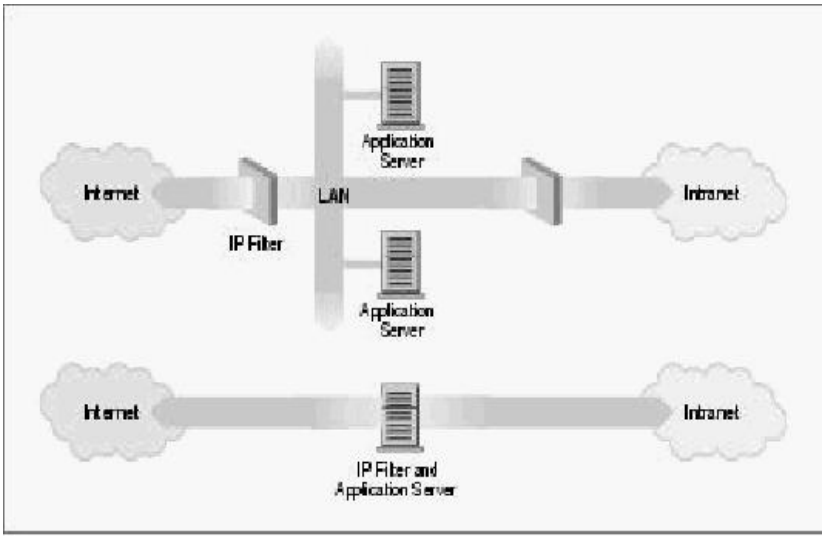


Figura II.9. Cortafuego entre dos redes

La figura muestra un cortafuego instalado entre dos redes para que el tráfico sea encaminado a través del cortafuego. El cortafuego puede de este modo proporcionar

control de acceso basado en los paquetes que se encaminan entre las redes. Un cortafuego es un dispositivo informático (por ejemplo un router ó un computador) que se utiliza para separar físicamente un dominio de red de otro. Los routers pueden controlar el tráfico en el nivel de red/transporte permitiendo ó denegando selectivamente el tráfico basado en dirección fuente/destino ó número de puerto.

Los computadores pueden controlar el tráfico en el nivel de aplicación. Estos cortafuegos aplican un conjunto de operaciones de filtrado de paquetes del nivel red/transporte. Un ejemplo sería un cortafuegos que realice decisiones de seguridad basadas en información en las cabeceras IP y TCP (por ejemplo dirección fuente y número de puerto).

2.2.9.1. ESTRUCTURA DE GRUPOS PARA LAS AMENAZAS A UN CORTAFUEGOS

A) GRUPO DE AMENAZAS GENÉRICAS

1) Personas no autorizadas pueden ganar acceso lógico al cortafuego. El término persona no autorizada se utiliza para cubrir todas aquellas personas que tienen ó pueden intentar ganar acceso lógico al cortafuegos pero no tienen autoridad para ganar acceso lógico al cortafuegos ó realizar operaciones sobre su información.

2) Personas no autorizadas pueden llevar a cabo ataques de "spoofing" de dirección de red (por ejemplo "spoofing" IP) desde una conexión de red a otra, atravesando el

cortafuego. El cortafuego proporciona control de acceso entre una ó más redes externas (no dignas de confianza) y una ó más redes internas (privadas, de confianza). La amenaza específica encontrada es que un sujeto de una red externa intente suplantar a un sujeto de la red interna.

3) Personas no autorizadas pueden realizar ataques a los servicios. Las amenazas específicas encontradas dependen de los protocolos que se permiten pasar a través del cortafuego. Un servicio que no puede ser accedido desde fuera de la red interna no plantea una amenaza. Las amenazas que no se originan del tráfico a través del cortafuego no se consideran específicamente en este estudio

4) Personas no autorizadas pueden realizar ataques del tipo encaminamiento fuente en el nivel de red. Varios protocolos del nivel de red permiten al originador de un paquete especificar el camino que el paquete va a seguir desde la fuente al destino. En algunas implementaciones de encaminamiento, si el encaminamiento fuente está indicado en la cabecera de protocolo, la función que procesa el protocolo se salta cualquier comprobación de reglas, de este modo se ofrece un camino no deseado para cruzar "por un túnel" el cortafuego realizando una función de encaminamiento.

5) Personas no autorizadas pueden realizar intentos de ingreso no detectados. Una persona no autorizada puede intentar repetitivamente diferentes ataques contra una red a proteger si no existe personal en la red atacada que se dé cuenta de que tales ataques están teniendo lugar.

6) Puede existir una falta de revisión del registro de auditoría. Incluso aunque se recojan los datos de auditoría, si estos datos no son revisados, bien debido a la cantidad de datos generados ó a la falta de herramientas de revisión adecuadas, un atacante puede no ser detectado mientras realiza intentos de penetración repetidos.

7) Un atacante puede modificar/degradar el registro de auditoría. Esta amenaza tiene dos facetas. En primer lugar, un atacante puede modificar directamente el registro de auditoría manipulándolo a través de un interface del cortafuego (por ejemplo, un protocolo de control específico que va sobre la red). En segundo lugar, un atacante puede averiar el cortafuego después de realizar un ingreso ó intento de acceso y si el registro de auditoría no está suficientemente protegido posiblemente puede perderse, de modo que se enmascaren las acciones del atacante.

8) Un atacante puede modificar la configuración del cortafuegos y otros datos de seguridad relevantes. Esta amenaza es similar a la anterior, salvo que los datos que son elegidos por un atacante son la configuración del cortafuego y otros datos de seguridad críticos.

9) Pueden ocurrir fallos de seguridad debido a defectos en el cortafuego. La seguridad ofrecida puede ser garantizada sólo hasta el punto de que todas las características de seguridad pueden ser confiables en cuanto a ser efectivas a la hora de contrarrestar las amenazas y operar correctamente y de forma fiable. Los agentes de amenazas pueden, a través del descubrimiento accidental ó la búsqueda dirigida, descubrir defectos en el cortafuego que pueden trastornar de modo que el funcionamiento de

las funciones de seguridad se cambie para su provecho. Dicho trastorno del cortafuego puede ocurrir durante la entrega e instalación. Durante el funcionamiento normal, potenciales atacantes también pueden desarrollar métodos con los que las funciones de seguridad pueden ser "minadas".

B) GRUPO DE AMENAZAS APLICADAS AL ENTORNO DE OPERACIÓN (ENTORNO, MEDIOS PROCEDURALES, RIESGOS POTENCIALES DEL SISTEMA)

1) Personal de administración del sistema hostil ó descuidado ó intencionalmente negligente. Puesto que los administradores son los responsables de establecer las reglas de control de acceso y de monitorizar el registro de auditoría, podrán fácilmente saltarse los mecanismos de seguridad del cortafuego.

2) Usuarios hostiles de una red protegida (situados detrás del cortafuego) desean compartir información con usuarios de la red externa. Esta amenaza trata el caso en que un usuario de una red interna (protegida) desea enviar información de forma ilegítima a un usuario de una red externa. Puesto que este tipo de cortafuegos está diseñado específicamente para proteger las redes internas de las redes externas y no trata de comprobar el contenido del paquete, generalmente ser inefectivo contra estas clases de ataques.

3) Usuarios hostiles de una red protegida atacan a máquinas que son parte de la red protegida. Puesto que un cortafuego por definición sirve para proteger a los usuarios

de una red interna de los usuarios externos a la red, no puede proteger de los ataques no dirigidos contra el cortafuego.

4) Usuarios hostiles de una red protegida intentan realizar ataques sofisticados a los servicios y protocolos de alto nivel. Estos tipos de ataques eligen defectos de los niveles de protocolo (y servicios que utilizan dichos protocolos) por encima del nivel de transporte. El cortafuegos puede ser capaz de denegar completamente paquetes a servicios específicos, pero una vez que a los paquetes se les permite pasar, entonces pueden ser posibles los ataques a los servicios que son elegidos. El cortafuego no necesita verificar el contenido del paquete.

Se supone que las siguientes hipótesis específicas ó condiciones de utilización segura se asumen en un entorno operacional con cortafuegos de filtrado de paquetes del nivel red/transporte.

2.2.9.2. LAS CONDICIONES FÍSICAS

1) El cortafuego y la consola asociada directamente conectada es segura, es decir, el acceso se encuentra limitado sólo al personal autorizado.

2) El personal autorizado (los administradores) interactúan con el cortafuego sólo a través de consolas directamente conectadas, es decir, ningún "login de red" se permite a los administradores.

3) El cortafuegos no requiere para funcionar cambios de las propiedades operativas (por ejemplo, aplicaciones software, hardware) de la red interna ó de la red externa.

2.2.9.3. CONDICIONES DE TIPO PERSONAL

1) El cortafuegos sólo está diseñado para actuar como cortafuegos y no para proporcionar servicios adicionales de usuario (por ejemplo, "login") a cualquier usuario de la red interna ó externa. Sólo los administradores poseen acceso directo.

2) Los administradores se supone que no son hostiles y son de confianza para realizar sus funciones correctamente. La condición de tipo de conectividad es: El cortafuegos es el único dispositivo de interconexión entre las redes. Una configuración en la que dos redes una pública y otra privada se conecten a la vez por un cortafuego y por una conexión directa no está permitida.

2.2.10. CONFIGURACION DE LOS CORTAFUEGOS COMO SERVIDOR DNS

En Internet, el DNS (Domain Name Service) proporciona la correspondencia y traducción de los nombres de dominio a direcciones IP (por ejemplo: 130.206.100.1 representa la dirección IP del computador orion.deusto.es). Algunos cortafuegos se pueden configurar como servidores DNS primarios, secundarios ó caché. Decidir cómo gestionar los servicios DNS normalmente no es una decisión de seguridad. Muchas organizaciones utilizan una tercera parte, como un ISP (Internet Service Provider) para gestionar su DNS. En este caso, el cortafuegos puede utilizarse como un servidor DNS

cache, que mejora el rendimiento pero no necesita la organización mantener su propia base de datos DNS.

Si la organización decide gestionar su propia base de datos DNS, el cortafuego puede (pero no tiene porqué) actuar como el servidor DNS. Si el cortafuegos debe ser configurado como un servidor DNS (primario, secundario ó caché), es necesario que se tomen otras precauciones de seguridad.

Una ventaja de implementar el cortafuego como un servidor DNS es que puede configurarse para ocultar la información de los computadores internos de una organización. En otras palabras, con el cortafuego actuando como un servidor DNS, los computadores internos obtienen una visión no restrictiva de los datos DNS internos y externos. Los computadores externos no tienen acceso a la información relativa a las máquinas computadoras internas. Para el mundo exterior, todas las conexiones a cualquier computador de la red interna parecen haberse originado desde el cortafuego. Con la información de computadores oculta del exterior, un atacante no sabrá los nombres y direcciones de los computadores de las máquinas informáticas internas que ofrecen servicios a Internet. Una política de seguridad para ocultar el DNS para cortafuegos es: "Si el cortafuego opera como un servidor DNS, entonces debe configurarse para ocultar la información relativa a la red para que los datos de los computadores internos no se revelen al mundo exterior (Internet)".

2.2.11. INCONVENIENTES DE LOS CORTAFUEGOS

El mayor problema de los cortafuegos es que restringen mucho el acceso a Internet desde la red protegida. Básicamente, reducen el uso de la Internet al que se podría hacer desde un terminal. Tener que entrar en el cortafuego y desde allí realizar todo el acceso a Internet es una restricción muy seria. Programas como Netscape que requieren una conexión directa con internet, no funcionan desde detrás de un cortafuego. La solución a todos estos problemas es un Servidor Proxy.

2.2.12. MANTENIMIENTO DE CORTAFUEGOS

Dentro de las tareas de mantenimiento tenemos tres grandes categorías:

1) Mantenimiento.

2) Monitoreo del sistema.

3) Mantenerse actualizado.

2.2.12.1. MANTENIMIENTO

1) Respaldo del cortafuegos: Asegúrese de respaldar todas las partes de su cortafuegos, lo cual se refiere no sólo a las computadoras de usos múltiples que puede estar usando como anfitriones bastión o servidores internos sino, también, a los enrutadores u otros dispositivos de propósitos especiales. Por lo general no es sencillo reconstruir configuraciones de enrutadores, y su seguridad depende de tenerlos bien configurados.

Coloque en sus máquinas de usos múltiples un sistema de copias de respaldo automatizado; de preferencia, debe crear correo de confirmación cuando funcione de modo normal y mensajes completamente diferentes cuando detecte errores.

2) Administración de cuentas: El mantenimiento de las cuentas (agregar nuevas cuentas, quitar las viejas, caducar las contraseñas, etc.) es una de las tareas de mantenimiento que se descuidan con más frecuencia. En los sistemas de cortafuegos, es del todo crucial que las nuevas cuentas se agreguen correctamente, que las viejas se quiten con oportunidad y que las contraseñas se cambien de modo apropiado (véase la documentación de su propio sistema para saber cómo hacer todo esto).

3) Administración del espacio en disco: La información siempre se extiende hasta llenar todo el espacio disponible, aun en máquinas que casi no tienen usuarios. La gente deja cosas en rincones extraños del sistema, “de manera provisional”, y luego se quedan ahí, lo cual ocasiona más problemas de los que se imagina. Además de que puede requerir ese espacio de disco, esta chatarra de información le complica la respuesta incidental. Desafortunadamente, no hay un modo automático de hallar la chatarra; los seres humanos, en particular los administradores de sistemas que pueden escribir en cualquier parte del disco, son demasiado impredecibles. Otra persona debe revisarlo periódicamente. Es en especial efectivo que cada nuevo administrador de sistemas revise los discos; se dará cuenta de cosas a las que los antiguos administradores ya se han acostumbrado.

2.2.12.2. MONITOREO DEL SISTEMA

Otro aspecto importante del mantenimiento de los cortafuegos implica el monitoreo del sistema. El monitoreo sirve para indicarle varias cosas:

¿Está comprometido su cortafuego?

¿Qué clases de ataques se han intentado contra él?

¿Funciona adecuadamente?

¿Puede su cortafuego proporcionar el servicio que sus usuarios necesitan?

Mecanismos de monitoreo para propósitos especiales: La mayor parte del monitoreo se realizará usando las herramientas y el registro proporcionado por las partes ya existentes de su cortafuegos, pero le puede parecer conveniente tener algunos mecanismos de monitoreo dedicados. Por ejemplo, tal vez desee instalar una estación de monitoreo en su red de perímetro a fin de que pueda asegurarse de que sólo los paquetes que espera pasen a través de ella. Puede usar una computadora de propósitos generales con software para monitoreo de red, o puede usar un mecanismo analizador de red de propósitos especiales.

2.2.12.3. MANTENERSE ACTUALIZADO

Este es el último punto importante del mantenimiento de los cortafuegos. Es obvio que debe mantener actualizado su sistema, pero antes de que pueda hacerlo debe mantenerse actualizado el propietario del sistema

Manténgase actualizado usted mismo: La parte más difícil del mantenimiento de los cortafuegos es estar al corriente de los continuos avances en este campo. Todos los días ocurren cosas nuevas; se descubren y explotan nuevos errores; se llevan a cabo ataques nuevos; están disponibles más accesorios y arreglos para sus sistemas, así como herramientas nuevas. Mantenerse actualizado con todos estos cambios puede ser, sin duda, la parte que más tiempo absorba del trabajo del administrador de cortafuegos. Para mantenerse actualizado puede buscar noticias, revistas especializadas y foros profesionales.

Cómo mantener sus sistemas actualizados: Si se preocupa por mantenerse actualizado a sí mismo, entonces mantener sus sistemas actualizados es una labor sencilla. Sólo debe estudiar cualquier problema nuevo sobre el que escuche, tan pronto como sepa de él.

Debe ser capaz de recabar información de las fuentes descritas en la sección previa a fin de decidir si un problema lo es o no para su sitio. Tenga en cuenta que no siempre podrá determinar de inmediato si un problema lo es para su sitio; puede tomar algunas horas o días para que la información que necesite llegue a sus manos. Tal vez deba hacer un juicio personal sobre un problema específico en ausencia de información sólida, basado sólo en reportes vagos sobre el problema y sus consecuencias. Su forma de proceder será determinada por sus circunstancias particulares. Éstas incluyen el problema potencial, qué puede hacer por él de modo realista, qué tanto le preocupa a su sitio la seguridad contra la disponibilidad y conveniencia, etc. La precaución implicaría bloquear el problema si es posible que le concierna.

Por otro lado, la conveniencia implicaría tomar un lapso de espera hasta que esté del todo seguro que el problema le atañe.

2.2.13. CONSIDERACIONES FINALES

El problema fundamental es que Internet no se diseñó para ser muy seguro. Algunos de los problemas inherentes con las versiones actuales de TCP/IP son:

1) **Fácil escucha clandestina y falsificación:** la mayor parte del tráfico Internet no se encuentra cifrada. El Correo Electrónico, las passwords y las transferencias de ficheros se pueden monitorizar y capturar utilizando fácilmente el software disponible.

2) **Los servicios TCP/IP son vulnerables:** Un conjunto de servicios TCP/IP no están diseñados para ser seguros y pueden ponerse en peligro por intrusos con ciertos conocimientos; los servicios utilizados para testear son particularmente vulnerables.

3) **Falta de política de seguridad**: Muchas organizaciones se encuentran configuradas, no intencionalmente, con acceso Internet a todo el mundo sin tener en cuenta los posibles abusos desde Internet. Muchas organizaciones permiten más servicios TCP/IP de los que son necesarios para sus operaciones y no intentan limitar el acceso a la información acerca de sus computadores que puede resultar valiosa para los intrusos.

4) **Complejidad de la configuración**: Los controles de acceso de seguridad a los computadores suelen ser complejos de configurar y monitorizar; los controles que se configuran incorrectamente de forma accidental pueden dar lugar a accesos no autorizados peligrosos.

De acuerdo con un informe de la Consultora Datapro, sólo el 46% de las Empresas Españolas disponen de una política de seguridad para sus sistemas de información. En Europa, el porcentaje asciende al 69%. El propósito de una política de seguridad es decidir la forma en que una organización toma medidas para protegerse. Una política de seguridad generalmente presenta tres aspectos:

1) Una política general que establece el enfoque a la seguridad.

2) Las reglas específicas que son el equivalente de la política específica del sistema. Las reglas definen lo que está ó no permitido. Las reglas pueden ser apoyadas por procedimientos y otras guías.

3) El enfoque técnico ó análisis que soporta la política general y las reglas específicas. Para que la política de seguridad sea efectiva sus diseñadores deben tener en cuenta los compromisos/concesiones que se realizan (muchas soluciones de seguridad limitan la funcionalidad para poder incrementar el grado de seguridad, se suele cumplir que a mayor seguridad mayor dificultad de uso, etc.). La política de seguridad debe sincronizarse con otras cuestiones de política relacionadas. Una política de seguridad puede estructurarse según: su destino, grado de robusted en:

- Para los usuarios.
- Para los administradores/gestores.
- Requisitos técnicos.
- Bajo riego.
- Riesgo medio.
- Alto riesgo, etc.

TABLA II.I. SERVIDORES CORTAFUEGOS

HERRAMIENTA	DESCRIPCIÓN	CARACTERÍSTICAS
PC Tools Firewall Plus	Potente cortafuegos personal para Windows® que protege su equipo al evitar que los usuarios no autorizados puedan acceder a su sistema a través de Internet o de otra red. El seguimiento de las aplicaciones con conexión a la red permite que Firewall Plus impida que los troyanos, backdoors, capturadores de teclado y otros programas malignos dañen su equipo y se hagan con sus datos privados. Se basa en una avanzada tecnología diseñada especialmente para usuarios expertos y no expertos. Al instalarlo, se activa automáticamente una potente protección contra ataques y riesgos conocidos.	Sistema operativo: WinXP/Vista/7 TAMAÑO : 10,2 MB (10.702.992 bytes) IDIOMA: Español y _Otros. Permite Especificar: - Las aplicaciones que pueden acceder a Internet y cuáles pueden entrar en el ordenador. - Configurar puertos, aplicar diversos niveles de seguridad según mejor

	Además, los usuarios experimentados pueden optar por crear sus propios conjuntos de reglas para los filtros, incluido el protocolo Ipv6, para adaptar la protección de sus redes. Lo único que tiene que hacer es instalar el programa para que, de manera inmediata y automática, se active la protección permanente.	convenga, - Controlar la continua actividad de red que se produzca en el ordenador, denegar conexiones específicas, y otras muchas opciones típicas de un buen programa cortafuegos.
ZoneAlarm Pro	Es una utilidad de seguridad en Internet y cortafuegos (firewall) que permitirá detectar todos los accesos a/de Internet en su computador y tener el control de qué programas tienen acceso, y de qué tipo, a Internet. Incluye varios servicios de seguridad que le resultarán fáciles de usar; protección global: cortafuegos, bloqueo de Internet, niveles y zonas de seguridad asignadas dinámicamente. El cortafuegos controla la puerta de entrada a su computador, permitiendo tráfico que	Sistema operativo: WinXP/Vista/7 TAMAÑO : 262 KB (268.680 bytes) IDIOMA : Español y Otros

	espera o haya iniciado. Además, con el modo de cautela "Stealth" activado, su computador será invisible a Internet y los potenciales intrusos.	
Look 'n' Stop	Look´n´Stop es un potente firewall que protege su computador contra intentos de acceder a él vía Internet. Permite filtrar todo el tráfico de datos y bloquear fácilmente cualquier acción sospechosa de ser un intento de infiltrarse. Posee los ataques más comunes bloqueados de antemano. Ha conseguido superar con éxito las pruebas más duras a las que son sometidos los firewall por las publicaciones especializadas en seguridad.	Sistema operativo: WinXP/Vista/7 TAMAÑO : 1,09 MB (1.152.512 bytes) IDIOMA : Español y Otros
Kerio WinRoute Firewall.	Potente cortafuegos que se destaca sobre todo por su gran versatilidad, seguridad y control de acceso del usuario, estando especialmente diseñado para redes	- Una de las principales características de Kerio WinRoute Firewall es que soporta un control total sobre el tráfico en la red,

	corporativas, protegiendo de toda clase de ataques externos por parte de hackers y del acceso de virus. También es destacable que restringe el acceso a sitios web dependiendo de su contenido.	y sobre todo una muy eficiente protección en toda clase de sistemas operativos aparte de Windows (Linux, Mac, etc.). A destacar también su capacidad para soportar todo tipo de conexión (ADSL, MODEM, wireless, etc.) adaptándose a cualquier tipo de protocolos de red existente
Agnitum Outpost Firewall Pro	Impide que nadie invada la intimidad de su computador sin consentimiento. Este firewall de Agnitum Outpost es el primero en usar una tecnología basada en plug-ins. Incluye plug-ins de ejemplo para mostrar la eficacia de este sistema en tareas como detección de intrusos, filtros, vigilancia del correo	Sistema operativo: Win2k/XP/2003/Vista TAMAÑO : 26,9 MB (28.264.448 bytes) IDIOMA : Español y Otros

	electrónico, bloqueo anti spam (elimina banners y pop-ups) y control de privacidad. Destaca por utilizar los últimos sistemas de seguridad disponibles y por proporcionar protección desde el preciso instante en el que se instale.	
Sunbelt Kerio Personal Firewall	Esta aplicación construye virtualmente un "muro" entre su computador e Internet, evitando así posibles ataques de otros usuarios con intenciones más bien poco amistosas. Está diseñado para proteger Su sistema tanto de otros ordenadores conectados en red local, como de ataques procedentes de sistemas remotos, controlando el tráfico de datos de entrada y salida y bloqueando todos aquellos intentos de acceso o de comunicación que el usuario no permita.	Sistema operativo: Win2000/XP/Vista/7 TAMAÑO : 5,72 MB (6.000.608 bytes) IDIOMA : Español y Otros
McAfee Personal	El cortafuegos permanece residente en la bandeja del	**Sistema Operativo:** 98 NT ME 2000

Firewall Plus	sistema, pudiendo acceder en cualquier momento a todas sus funciones, pero sin interferir en su trabajo cuando no se lo requiera. McAfee Personal Firewall notificará puntualmente todas y cada una de las conexiones de entrada que se intenten efectuar a tu PC. Las opciones de configuración son interminables, y se encontrar el funcionamiento del cortafuegos a la medida: Varios niveles de seguridad, avisos y alarmas, listas de direcciones IP permitidas y bloqueadas, comprobación del tráfico, etc.	XP **Idiomas:** **Licencia:** Shareware **Tamaño:** 6Mb
Sygate Personal Firewall	Es un excelente cortafuegos para su computador, que esté conectado a Red LAN, VPN o a Internet. Protege contra troyanos, spyware, gusanos y otros conocidos y desconocidos peligros, además previene contra el uso no autorizado de aplicaciones maliciosas, así como	**Sistema Operativo:** 95 98 NT ME 2000 XP Vista **Idiomas:**

	accesos de otros usuarios no autorizados a través de los distintos tipos de red. En todo momento, permite conocer las conexiones entrantes y salientes de nuestro computador, por lo que fácilmente podremos visualizar si hay algún acceso sospechoso, con el objetivo de cerrarlo inmediatamente.	**Licencia:** Freeware **Tamaño:** 9Mb
Comodo Firewall Pro	Es una utilería poderosa que incluye un excelente **firewall** con opciones avanzadas, y además trae una herramienta **anti-malware** llamada **Defense+**, la cual es opcional al momento de la instalación.	**Licencia: Gratis**

Tabla II.I. Ejemplos de Servidores Cortafuegos

2.3. PROXY

2.3.1. CARACTERÍSTICAS

Un proxy es una aplicación o un dispositivo hardware que hace de intermediario entre los usuarios, normalmente de una red local, e Internet.
Lo que hace realmente un proxy es recibir peticiones de usuarios y redirigirlas a Internet. La ventaja que presenta es que con una única conexión a Internet podemos conectar varios usuarios.

Normalmente, un proxy es a su vez un servidor de caché. La función de la caché es almacenar las páginas web a las que se accede más asiduamente en una memoria. Así cuando un usuario quiere acceder a Internet, accede a través del proxy, que mirará en la caché a ver si tiene la página a la cual quiere acceder el usuario. Si es así le devolverá la página de la caché y si no, será el proxy el que acceda a Internet, obtenga la página y la envíe al usuario. Con la caché se aceleran en gran medida los accesos a Internet, sobre todo si los usuarios suelen acceder a las mismas páginas.

El proxy es transparente al usuario, el usuario tendrá que configurar su navegador diciéndole que accede a Internet a través de un proxy (deberá indicar la dirección IP del proxy y el puerto por el que accede), pero una vez realizado esto, el usuario actuará de la misma manera que si accediera directamente a Internet.

Los últimos proxies que han aparecido en el mercado realizan además funciones de filtrado, como por ejemplo, dejar que un usuario determinado acceda a unas

determinadas páginas de Internet o que no acceda a ninguna. Con esta función podemos configurar una red local en la que estarán usuarios a los que se les permita salir a Internet, otros a los que se les permita enviar correo, pero no salir a Internet y otros que no tengan acceso a Internet. Esta característica muchas veces hace que se confundan con un cortafuego

Lo importante de los servidores proxy es que, bien configurados, son completamente seguros. No dejan que nadie entre a través de ellos.

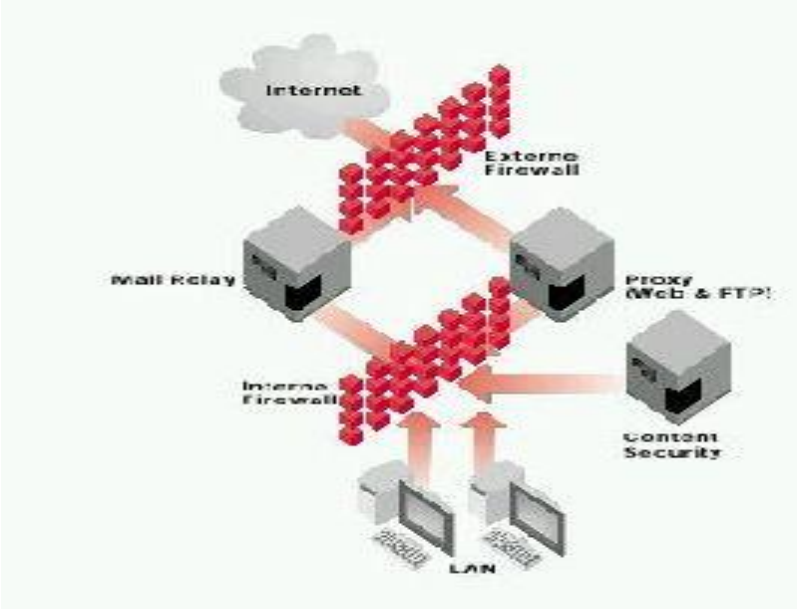


Figura II.10. Proxy

2.3.2. VENTAJAS DEL USO DE PROXY

- Los servicios proxy permiten a los usuarios acceder de forma “directa” a internet.
- Los servicios proxy son buenos para la contabilidad del sistema (contabilidad de transferencia de datos transferidos)

3.3.3. DESVENTAJAS DEL USO DE PROXY

- Los servicios proxy son más lentos que los servicios no proxy.
- Los servicios proxy podrían requerir servidores diferentes para cada servicio.
- Los servicios proxy por lo general requieren modificaciones a los clientes, a los procedimientos o a ambos.
- Los servicios proxy no funcionan para algunos servicios.
- Los servicios proxy no protegen de todas las debilidades de los protocolos.

3.3.4. DIFERENCIAS ENTRE UN CORTAFUEGO Y UN PROXY

El proxy y el firewall son diferentes, pero deberían estar siempre combinados. El proxy se usa para redirigir las peticiones que recibe de varios usuarios a Internet de forma transparente y se encarga de devolverles las respuestas (las páginas web). También se puede utilizar para FTP, POP3, SMTP, IMAP, TELNET, etc.

El firewall sin embargo, es únicamente un método de protección de la red local o de un ordenador personal, con el que podemos cerrar o dejar abiertos ciertos puertos, IPs, aplicaciones, etc.

2.3.5 SERVIDORES PROXY

Un servidor proxy es en principio un equipo que actúa como intermediario entre los equipos de una red de área local (a veces mediante protocolos, con excepción del

protocolo TCP/IP) e Internet, son un invento que permite el acceso directo a Internet desde detrás de un cortafuego.

Generalmente el servidor proxy se utiliza para la Web. Se trata entonces de un proxy HTTP. Sin embargo, puede haber servidores proxy para cada protocolo de aplicación (FTP, etc.).

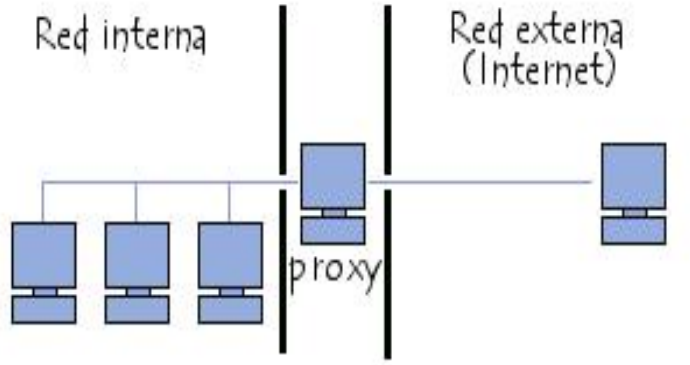


Figura II.11. Uso de servidores proxy

2.3.5.1. PRINCIPIO OPERATIVO DE UN SERVIDOR PROXY

El principio operativo básico de un servidor proxy es bastante sencillo: se trata de un servidor que actúa como "representante" de una aplicación efectuando solicitudes en Internet en su lugar. De esta manera, cuando un usuario se conecta a Internet con una aplicación del cliente configurada para utilizar un servidor proxy, la aplicación primero se conectará con el servidor proxy y le dará la solicitud. El servidor proxy se conecta entonces al servidor al que la aplicación del cliente desea conectarse y le envía la

solicitud. Después, el servidor le envía la respuesta al proxy, el cual a su vez la envía a la aplicación del cliente.

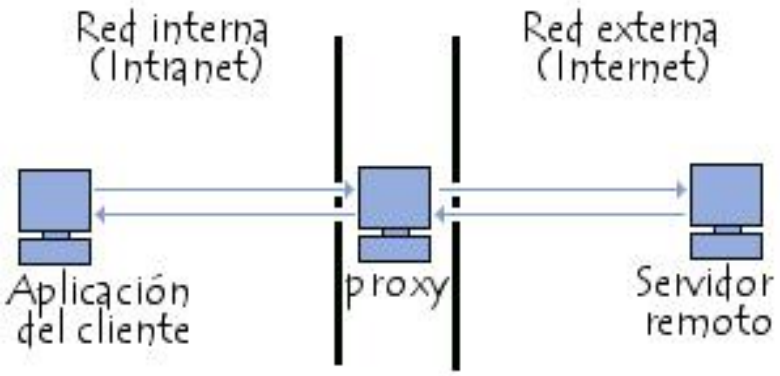


Figura II.12. Principio operativo de servidores proxy

2.3.5.2. CARACTERÍSTICAS DE UN SERVIDOR PROXY

En lo sucesivo, con la utilización de TCP/IP dentro de redes de área local, la función de retransmisión del servidor proxy está directamente asegurada por pasarelas y routers. Sin embargo, los servidores proxy siguen utilizándose ya que cuentan con cierto número de funciones que poseen otras características.

2.3.5.3. ALMACENAMIENTO EN CACHÉ

La mayoría de los proxys tienen una caché, es decir, la capacidad de guardar en memoria (“en caché”) las páginas que los usuarios de la red de área local visitan comúnmente para poder proporcionarlas lo más rápido posible. De hecho, el término

"caché" se utiliza con frecuencia en informática para referirse al espacio de almacenamiento temporal de datos (a veces también denominado "búfer").

Un servidor proxy con la capacidad de tener información en caché (neologismo que significa: poner en memoria oculta) generalmente se denomina servidor "proxy-caché". Esta característica, implementada en algunos servidores proxy, se utiliza para disminuir tanto el uso de ancho de banda en Internet como el tiempo de acceso a los documentos de los usuarios. Sin embargo, para lograr esto, el proxy debe comparar los datos que almacena en la memoria caché con los datos remotos de manera regular para garantizar que los datos en caché sean válidos.

2.3.5.4. FILTRADO

Por otra parte, al utilizar un servidor proxy, las conexiones pueden rastrearse al crear registros de actividad (logs) para guardar sistemáticamente las peticiones de los usuarios cuando solicitan conexiones a Internet.

Gracias a esto, las conexiones de Internet pueden filtrarse al analizar tanto las solicitudes del cliente como las respuestas del servidor. El filtrado que se realiza comparando la solicitud del cliente con una lista de solicitudes autorizadas se denomina lista blanca; y el filtrado que se realiza con una lista de sitios prohibidos se denomina lista negra. Finalmente, el análisis de las respuestas del servidor que cumplen con una lista de criterios (como palabras clave) se denomina filtrado de contenido.

2.3.5.5. AUTENTICACIÓN

Como el proxy es una herramienta intermediaria indispensable para los usuarios de una red interna que quieren acceder a recursos externos, a veces se lo puede utilizar para autenticar usuarios, es decir, pedirles que se identifiquen con un nombre de usuario y una contraseña. También es fácil otorgarles acceso a recursos externos sólo a las personas autorizadas y registrar cada uso del recurso externo en archivos de registro de los accesos identificados.

Este tipo de mecanismo, cuando se implementa, obviamente genera diversos problemas relacionados con las libertades individuales y los derechos personales.

2.3.5.6. SERVIDORES DE PROXY INVERSOS

Un proxy inverso es un servidor proxy-caché "al revés". Es un servidor proxy que, en lugar de permitirles el acceso a Internet a usuarios internos, permite a usuarios de Internet acceder indirectamente a determinados servidores internos.

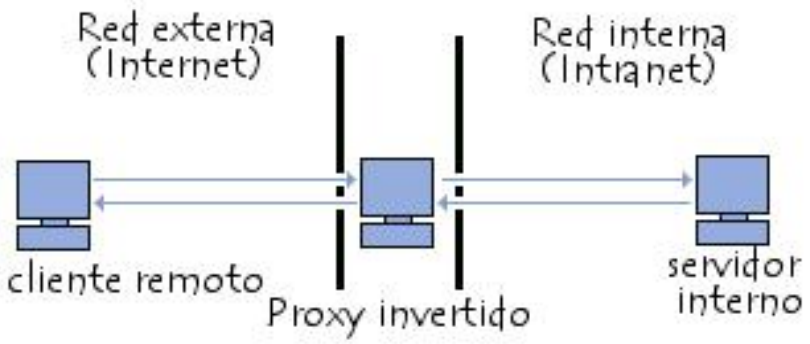


Figura II.13. Servidores proxy inversos

El servidor de proxy inverso es utilizado como un intermediario por los usuarios de Internet que desean acceder a un sitio web interno al enviar sus solicitudes indirectamente. Con un proxy inverso, el servidor web está protegido de ataques externos directos, lo cual fortalece la red interna. Además, la función caché de un proxy inverso puede disminuir la carga de trabajo del servidor asignado, razón por la cual se lo denomina en ocasiones acelerador de servidor.

Finalmente, con algoritmos perfeccionados, el proxy inverso puede distribuir la carga de trabajo mediante la redirección de las solicitudes a otros servidores similares. Este proceso se denomina equilibrio de carga.

2.3.5.7. VENTAJAS DE UN SERVIDOR PROXY

Un servidor Proxy actúa como intermediario entre el programa cliente (Netscape, Mozilla, Internet Explorer, u otro) y el servidor web que contiene la información que queremos obtener. Su función consiste en almacenar páginas de Internet, gráficos, fotos, archivos de música, para que la próxima vez que se pida el mismo objeto no se deba acceder de nuevo al servidor web que lo alojaba, sino que se sirva directamente desde su memoria o lo que es lo mismo desde su caché.

- En cuanto a las ventajas, un servidor Proxy con caché en principio realiza la misma función que el resto de caches privados como los que utilizan los navegadores, pero de manera compartida por un conjunto grande de usuarios que acceden a través de él. Al tratarse de un almacenamiento compartido es más probable que varios usuarios pidan los mismos objetos consiguiéndose de este

modo una reducción en los tiempos de espera para el usuario final. Ésta no es la única ventaja de disponer de éste sistema, a continuación se indican otras ventajas a considerar.

- Puede controlar el acceso a Internet prohibiendo por ejemplo la entrada a determinadas páginas web por su contenido erótico o por cualquier otro motivo, ya que un servidor Proxy puede realizar simplemente la función de pasarela sin realizar caché.

- El coste del software y su instalación tienen un precio prácticamente nulo para acceder a Internet mediante una sola línea, a diferencia del coste de usar cualquier router.

- Un servidor Proxy además actúa como una barrera (firewall) que limita el acceso a la red desde el exterior.

2.3.5.8. DESVENTAJAS DE UN SERVIDOR PROXY

Utilizar un servidor Proxy-Caché en principio puede parecer una gran ventaja ya que se disminuye el tiempo de acceso al contenido deseado y además el servidor que aloja el contenido no recibe tantas peticiones, pero no todo son ventajas, a continuación se indican posibles inconvenientes:

- Debido a que el funcionamiento de un Proxy no es conocido por todos los usuarios o webmasters, puede suponer un inconveniente al visualizar las páginas ya que éstas pueden no mostrarse actualizadas si no entendemos su funcionamiento.

- Un diseñador de páginas web puede indicar en el contenido de su web que los navegadores no hagan una caché de sus páginas, pero este método no funciona para un Proxy (a menos que se utilicen lenguajes como PHP).

- El hecho de acceder a Internet a través de un Proxy, en vez de mediante conexión directa, impide realizar operaciones avanzadas a través de algunos puertos o protocolos, aunque también es cierto que algunas pueden habilitarse tal como veremos más adelante.

- Almacenar las páginas y objetos que los usuarios solicitan puede suponer una violación de la intimidad para algunas personas, aunque también es cierto que desde el punto de vista de las empresas es una manera de controlar las actividades de sus trabajadores.

2.3.5.9. CONFIGURACIÓN DE UN SERVIDOR PROXY

Sin duda, el proxy más utilizado es Squid, un software de uso libre y gratuito, disponible para diversas plataformas que incluyen a Windows y Linux. En Windows,

existen diferentes programas para configurar un servidor proxy en una red de área local a un bajo costo:

- Wingate es la solución más común (pero no es gratuito)
- La configuración de un proxy con un servidor Jana cada vez es más común
- Windows 2000 incluye Microsoft Proxy Server (MSP), que funciona con Microsoft Proxy Client.

Algunos servidores proxy y sus características se indican en el listado siguiente:

TABLA II.II. SERVIDORES PROXY PARA WINDOWS

HERRAMIENTA	DESCRIPCIÓN	CARACTERÍSTICAS
WinProxy 6.1 R1c	Servidor que permite el acceso a Internet en diferentes ordenadores, con una sola conexión, en red local. Aporta una gran seguridad y limita sitios Webs. Tiene integrado: Anti-Spyware, Anti-Phishing, Antivirus, Antispam, Firewall y filtros para webs.	- Shareware
FreeProxy 3.81 Build 1526	Realiza conexiones a internet con diferentes ordenadores a través de un único punto de acceso. Permite acceso a Internet en el tiempo y a las webs que se desee.	-- Libre.
ChProxy 2.0	ChProxy es un proxy HTTP de Internet gratuito. Con este programa se podrá hacer que una red de trabajo	- Libre

	entera acceda a Internet con sólo una cuenta de Internet; ChProxy integra funciones de directorios locales, sitios Web locales, lectura de RSS, motores de búsqueda múltiples, soporte para caché volátil y persistente, bloqueo de ventanas emergentes, lista blanca y lista negra. El programa es fácil de configurar y utilizar.	
AnalogX Proxy 4.14	Servidor que permite compartir única conexión a internet en una red local.	- Libre
ezProxy 2.7.1 Build20060218	Brinda conexión a Internet a todos los ordenadores que se encuentren en una misma red local por medio de un solo acceso. Cuenta con un buen soporte.	- Shareware
All Aboard! SE 2.5	Permite conectar múltiples ordenadores a internet a través de una única conexión. Soporta muchos tipos de redes y conexiones de internet. Incluye una opción	- Shareware

	para monitoreo.	
Intergate 9.02	InterGate combina lo mejor en tecnología NAT, filtrado de Internet y DHCP es un firewall seguro; el programa ofrece una manera rápida, fácil y segura de compartir una conexión sencilla a Internet a través de tu red de área local	- Libre, demo
AllegroSurf 7.0.0.2	Comparte la única conexión de internet en una red LAN con este servidor Proxy, que además incluye firewall y mejoras para la velocidad de conexión.	- Shareware
Proxy+ 3.00	Servidor de proxy/firewall y servidor de correo que aumentará la seguridad de la LAN ya que separa eficientemente la red LAN de la Internet y le brinda acceso a Internet a todos los PC con una sola conexión. Tiene soporte para múltiples protocolos y servicios, opciones para restricciones de acceso,	- El uso es libre para redes de hasta 3 ordenadores.

	manejo y optimización de la caché de discos duros, y mucho más.	
Avirt Soho 4.3	Este programa permite que incorporar hasta cinco computadores a una sola conexión con Internet. Dispone de una caché para las páginas visitadas con mayor frecuencia y una función de protección de usuarios exteriores.	- Shareware
PPPshar Pro 1.9	Por medio de una conexión permite que cada ordenador tenga Internet de manera individual en tu red local.	- Shareware
GProxy 1.26	Permite que a través de un modem que todos los computadores en red local tengan acceso a Internet por medio de una sola conexión. La función siempre debe estar activa, de lo contrario se realiza una desconexión automática.	- Shareware

RideWay 2.40	Es una excelente utilidad que brinda la capacidad de incluir una gran cantidad de computadores para compartir la única conexión existente de Internet en red.	- Shareware
ProxyMail 4.3.2	Herramienta que te permite instalar en cada computador de una red local e-mail e internet, por medio de una única conexión.	- Demo

Tabla II.II. Ejemplos de Servidores Proxy

CAPITULO III

ESTUDIO DE HERRAMIENTAS PARA EL CONTROL DE ACCESO A INTERNET

3.1. SQUID: SERVIDOR PROXY CACHE.

3.1.1. INTRODUCCIÓN

Squid es un servidor web proxy-caché con licencia GPL cuyo objetivo es funcionar como proxy de la red y también como zona caché para almacenar páginas web, entre otros. Se indica las principales características y funcionalidades de este potente servicio de amplia difusión en entornos GNU/Linux.

3.1.2 SERVIDOR PROXY-CACHÉ

¿Qué es un servidor proxy-caché?: Es un servidor situado entre la máquina del usuario y otra red (a menudo Internet) que actúa como protección separando las dos

redes y como zona caché para acelerar el acceso a páginas web o poder restringir el acceso a contenidos.

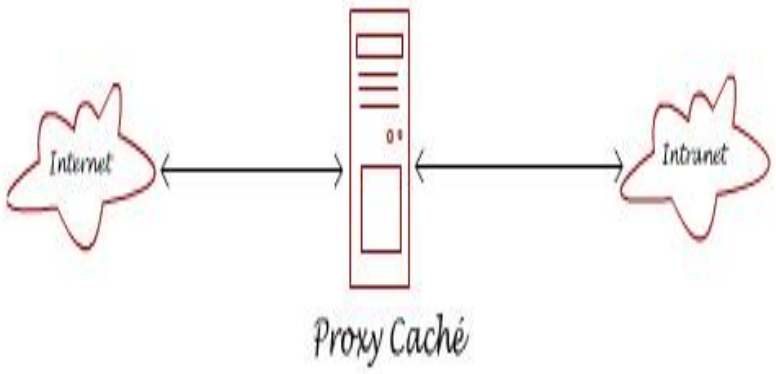


Figura III.14. Squid servidor proxy cache

La función de un servidor proxy es centralizar el tráfico de una red local hacia el exterior (Internet). Sólo el equipo que incorpora el servicio proxy debe disponer de conexión a Internet y el resto de equipos salen a través de él.

Como las peticiones hacía Internet de los equipos de la red local son interceptadas por el servidor proxy, éste puede realizar una tarea de filtrado de accesos, impidiendo aquellos destinos que estén expresamente prohibidos en los archivos de configuración del servicio. Squid no es un filtro de contenidos pero puede actuar como tal.

En los laboratorios se suele utilizar este servicio porque permite llevar un control sobre la actividad de la red hacia el exterior del aula. En este caso lo usual es que el equipo que hace la función de servidor proxy disponga de dos interfaces de red. Una de ellas es utilizada para atender a la red local y la otra proporciona la conexión con Internet. Las peticiones de páginas web que se realizan desde el aula son interceptadas por la interfaz

interna y reenviadas a la interfaz externa si cumplen los requisitos establecidos desde el servicio proxy.

Hay que tener en cuenta que la mayoría de los servidores web permiten la configuración como proxy-caché (Apache, IIS, etc.), pero Squid sólo es un proxy y no puede servir páginas por sí mismo.

Al indicar que Squid también funciona como caché significa que está guardando copia de los datos obtenidos de otras peticiones y de esa forma acelera el acceso a estos datos si se producen peticiones similares. Sólo se accederá de nuevo a las páginas originales cuando se detecte que se han producido modificaciones, es decir los datos almacenados difieren de los datos en el servidor web de origen.
Normalmente no existe una sola caché, sino que se tienen varios servidores (en máquinas diferentes) relacionados entre sí mediante una estructura en árbol.

3.1.3 FUNCIONES

Como resumen, las principales funciones de Squid son las siguientes:

- Permite el acceso web a máquinas privadas (IP privada) que no están conectadas directamente a Internet.
- Controla el acceso web aplicando reglas.
- Registra el tráfico web desde la red local hacia el exterior.
- Controla el contenido web visitado y descargado.

- Controla la seguridad de la red local ante posibles ataques, intrusiones en el sistema, etc.
- Funciona como una caché de páginas web. Es decir, almacena las páginas web visitadas por los usuarios y de esta manera las puede enviar a otros usuarios sin tener que acceder a Internet de nuevo.
- Guarda en caché las peticiones DNS e implementa una caché para las conexiones fallidas.
- Registra logs de todas las peticiones cursadas.
- Soporta el protocolo ICP que permite integrar cachés que colaboran y permite crear jerarquías de cachés y el intercambio de datos.

3.1.4. VENTAJAS

Como consecuencia de estas funciones, la implantación de un servidor proxy-caché en una red proporciona las siguientes:

- **Reduce los tiempos de respuesta.**

  Si la página web que se solicita está en la caché del servidor, ésta se sirve sin necesidad de acceder de nuevo al servidor original, con lo cual se ahorra tiempo.

- **Disminuye el tráfico en la red y el consumo de ancho de banda.**

  Si la página web está almacenada en la caché del servidor, la petición no sale de la red local y no será necesario hacer uso de la línea exterior consiguiendo así un ahorro en la utilización del ancho de banda.

- **Cortafuegos.**

  Cuando se utiliza un servidor proxy-caché, éste comunica con el exterior, y puede funcionar como cortafuegos, lo cual aumentará la seguridad del usuario respecto a la información a la que se acceda.

- **Filtrado de servicios.**

  Es posible configurar el servidor proxy-caché dejando sólo disponibles aquellos servicios (HTTP, FTP, u otro) que se consideren necesarios, impidiendo la utilización del resto.

3.1.5. INSTALACIÓN

El paquete incluido en Edubuntu Feisty Fawn es squid-2.6.5 Estable. Para instalar el servicio utilizar la herramienta Synaptic (Sistema -> Administración -> Gestor de paquetes Synaptic):

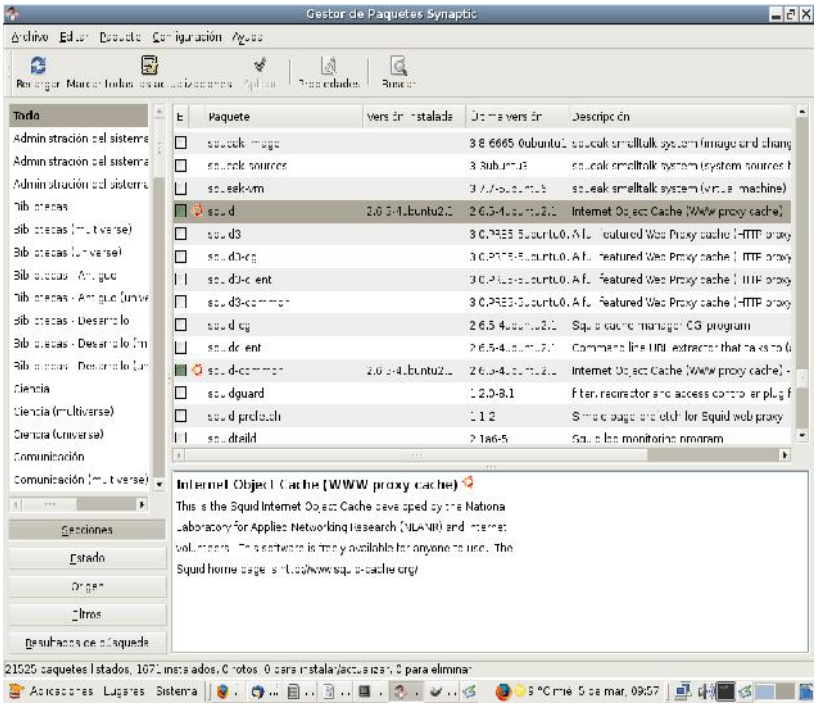


Figura III.15. Instalación de Squid

Seleccionamos el paquete, pulsamos el botón derecho para marcar para instalar y aplicamos los cambios (botón Aplicar).

3.1.6. COMPONENTES

Los componentes de Squid se instalan en los siguientes directorios:

TABLA III. IIII. COMPONENTES

Archivos/Directorios	Descripción
/usr/sbin/	Directorio del ejecutable.
/var/run/	Archivo con el PID del proceso.
/var/log/squid/	Directorio de logs. Relacionado con la directiva access_log.
/var/spool/squid/	Directorio caché. Relacionado con cache_dir.
/etc/squid/	Archivos de configuración.
/usr/lib/squid/	Complementos.
/etc/rc.d/	Scripts de arranque.
/usr/share/doc/squid/	Documentación.

Tabla III.III. Directorios de instalación de Squid

3.1.7. CONFIGURACIÓN BÁSICA

En el servidor habrá que:

- Determinar el espacio en disco dedicado al servidor proxy-caché.
- Configurar el propio servidor a nivel de puerto, directorios, usuarios, etc.
- Arrancar el servicio

En el cliente para que utilice el servidor proxy habrá que realizar una:

- Configuración manual (servidor, protocolos y puerto)
- Configuración automática utilizando un archivo proxy.pac

La utilización del proxy-caché requiere configurar el navegador para indicar que la conexión a Internet no es directa, sino a través del proxy. Suele estar en el menú principal Ver>Preferencias.

El archivo de configuración de SQUID es /etc/squid/squid.conf. Una configuración básica debe incluir los siguientes parámetros:

- **CACHE_EFFECTIVE_USER / GROUP**

  Por problemas de seguridad es preferible que Squid y sus procesos asociados se ejecuten como usuario y grupo proxy. Este usuario deberá ser el propietario del directorio caché y el directorio de logs.

  cache_effective_user proxy

  cache_effective_group proxy

  Al escribir no debe haber ningún blanco en la primera columna.

- **HTTP_PORT**

Por defecto Squid atiende peticiones por el puerto 3128 pero también se puede utilizar el 8080. Se puede cambiar el puerto e incluso Squid puede escuchar por varios puertos a la vez.

```
http_port 3128
```

Si se quiere aumentar la seguridad, puede vincularse el servicio a una IP que sólo se pueda acceder desde la red local. Considerando que el servidor utilizado posee una IP 10.0.2.254, puede hacerse lo siguiente:

```
http_port 10.0.2.254:3128

http_port 10.0.2.254:8080
```

- **DNS_NAMESERVERS**

Indica las direcciones IP de los servidores DNS donde el servidor realizará las consultas de nombres.

```
dns_nameservers 10.0.2.254
```

En el ejemplo el propio servidor está resolviendo nombres.

- **CACHE_PEER**

Squid permite crear jerarquías de cachés. Puede haber proxys-cachés padres y hermanos. Si establecemos una jerarquía padre-hijo (parent), el padre debe proporcionar el objeto pedido tanto si está en la caché como si no lo está.

Para utilizar un proxy-caché padre éste tiene que darnos permiso para utilizar su línea externa y en el archivo de configuración se deberá indicar:

Sintaxis:

cache_peer servidor tipo http_port icp_port [opciones]

Ejemplo:

cache_peer nombre/IP parent 8080 0 no-query no-digest default

Si establecemos una jerarquía entre hermanos (sibling), el proxy hermano sólo sirve el objeto si lo tiene en caché, nunca irá a Internet a buscarlo. Esto sólo es útil para redes con proxys en el mismo nivel.

Donde:

8080 -> puerto HTTP del servidor remoto.

0 -> indica el puerto ICP del servidor remoto. Se utiliza cuando hay varios padres, para averiguar cuál de ellos tiene el objeto pedido. Si hay un solo padre se coloca un 0.

no-query -> desactiva la petición de paquetes ICP al padre.

no-digest -> no es necesario con un solo padre.

default -> Squid utilizará este servidor para todas las peticiones.

- **CACHE_MEM**

Establece la cantidad de memoria RAM dedicada para almacenar los bloques más solicitados. Si la cantidad de memoria necesaria para este tipo de objetos es mayor que la especificada en el parámetro cache_mem, Squid tomará la que le haga falta.

Es una buena norma asignar N/3, siendo N la RAM del equipo.

cache_mem 96 MB

- **CACHE_DIR**

Especifica el tamaño de la caché en disco duro. Por defecto 100MB. Se pueden especificar el nº de subdirectorios y el nº de niveles posibles dentro de cada subdirectorio.

cache_dir ufs /var/spool/squid 100 16 256

Esta línea indica una caché en disco de 100MB, con 16 subdirectorios de primer nivel que se pueden utilizar y 256 subdirectorios de segundo nivel.

- **ACL LISTA DE CONTROL DEL ACCESO**

Permite:

- Proteger al proxy de conexiones externas, evitando que se conecten clientes desconocidos que podrían saturar la conexión con el exterior.
- Proteger a los clientes de accesos a puertos peligrosos actuando como cortafuegos contra posibles ataques desde la web.
- Establecer una jerarquía de cachés.
- Establecer una red como conjunto de trabajo o máquinas individuales.
- A continuación, a cada ACL se le hace corresponder una Regla de Control de Acceso (http_access).

La sintaxis es: acl [nombre_lista] src [componentes_lista]

Donde:

src -> hace referencia al origen, es decir, a la IP de un cliente.

[componentes_lista] -> se pueden indicar valores IP de redes, con la máscara de red, o archivos cuyo contenido sean las IPs.

Ejemplo:

acl aula src 10.0.2.0/255.255.255.0

acl aula “/etc/squid/mi_red”

Donde el archivo /etc/squid/mi_red tendría las IPs de las máquinas del aula (una por línea).

Se pueden crear ACLs para impedir el acceso, desde el proxy, a ciertas páginas web:

acl web_denegadas dstdomain .chicas.com .sex.com

El parámetro acl también se utiliza para establecer las conexiones permitidas a través del proxy. Podemos limitar los puertos a los que puede conectarse para atender las peticiones mediante la lista “SSL_ports”. Para ello se utiliza el método CONNECT, que es una puerta para la conexión a otros servidores desde el proxy.

acl SSL_ports port 443 563

acl CONNECT method CONNECT

http_access deny !SSL_ports

http_access deny CONNECT !SSL_ports

En este caso se está permitiendo la conexión, mediante CONNECT, a los puertos SSL 443 y 563.

Se puede restringir la salida a Internet durante un período de tiempo. Por ejemplo, a las máquinas especificadas se les deja conectar desde las 9h de la mañana hasta las 17h de la tarde:

```
acl IP_permitidas src 10.0.2.5 10.0.2.8 10.0.2.11

acl horario time MTWHF 9:00-17:00 de lunes a viernes de 9 a 5

acl host2 src 10.0.2.2

acl mañana time 9:00-14:00
```

Las Listas de control de acceso sirven también para especificar URLs que contienen un texto en concreto y a las cuales no se quiere permitir el acceso. Para ello se crea un archivo /etc/squid/denegar.txt con un texto por línea y que deberá estar contenido en el nombre de la URL.

En el archivo de configuración /etc/squid/squid.conf se añade:

```
acl url_denegar url_regex "/etc/squid/denegar.txt"

http_access deny url_denegar
```

Si lo que se quiere es hacer el filtrado por algún contenido del path no por el nombre del host, hay que utilizar la entrada urlpath_regex y pasarle como argumento un archivo con las palabras a filtrar.

- **HTTP_ACCESS REGLA DE CONTROL DE ACCESO**

La regla de control de acceso define qué navegadores u otros proxys podrán acceder o no a Squid para hacer peticiones HTTP. Se aplica sobre la Lista de control de acceso ACL.

La sintaxis es: http_access [deny / allow] [lista_control_acceso]

Ejemplo: para la ACL acl aula "/etc/squid/mi_red" le correspondería

http_access allow aula

En la que permitimos el acceso a Squid a los equipos del aula.

Si dentro del aula hay equipos a los que no se quiere dar acceso se puede utilizar el caracter **!** para excluirlos. Para ello creamos otra ACL con las máquinas no permitidas y escribimos:

http_access allow aula !no_permitidos

Ejemplo completo:

Tenemos una red 10.0.2.0/255.255.255.0 de la que sólo ciertas IPs van a poder acceder a Squid. Creamos con estas IPs un archivo 'permitidos' y su ACL correspondiente:

acl permitidos src "/etc/squid/permitidos"

Una configuración básica bajo estas condiciones sería:

```
acl todo src 0.0.0.0/0.0.0.0

acl permitidos src “/etc/squid/permitidos”

acl web_denegadas dstdomain .chicas.com .sex.com

acl horario time MTWHF 9:00-17:00

acl mañana time 9:00-14:00

acl url_denegar url_regex “/etc/squid/denegar.txt”

http_access allow permitidos horario

http_access deny permitidos

http_access deny web_denegadas

http_access deny url_denegar

http_access deny todo
```

En este ejemplo:

Se crea una ACL 'todo' para cualquier IP.

Se crea una ACL para las IPs permitidas.

Se crea una ACL para seleccionar ciertas webs destino.

Se establecen horarios de conexión.

Se seleccionan URLs que cumplen ciertos patrones.

Las líneas http_access permiten o deniegan la conexión en función de la ACL sobre la que actúan.

La lectura se hace de arriba hacia abajo y se detiene en la primera coincidencia para permitir o denegar la conexión.

Si una línea http_access tiene más de un argumento se evalúan con un AND y con la siguiente línea http_access con un OR.

- **CACHE_MGR**

Este parámetro especifica la dirección de correo del administrador a la que se enviará un mensaje en el caso de que le ocurra algo a la caché.

cache_mgr webmaster

- **HTTPD_ACCEL**

Las peticiones de Internet de los usuarios se almacenan en la caché de Squid. Si otros usuarios solicita la misma petición y el elemento en caché no ha sufrido ninguna modificación, Squid muestra el de la caché y no vuelve a descargarlo de Internet con lo cual se aumenta la rapidez en la navegación.

Por ejemplo, para un proxy convencional, las opciones para proxy acelerado son:

httpd_accel_host virtual

httpd_accel_port 0

httpd_accel_with_proxy on

Donde:

- httpd_accel_host indica el nombre del servidor web que se quiere acelerar. Si se escribe 'virtual' se está indicando que se quiere acelerar más de un servidor.
- httpd_accel_port indica el puerto donde escucha el servidor que se quiere acelerar.
- httpd_accel_with_proxy permite al proxy trabajar como proxy y como acelerador al mismo tiempo ya que con la primera opción (httpd_accel_host) Squid deja de actuar como proxy.

3.1.8. UBICACIÓN DEL PROXY

La ubicación del cortafuegos respecto al proxy-caché tiene mucha importancia de cara a su configuración.

¿Qué posibilidades tenemos?

- Proxy-caché dentro de la zona protegida
- Proxy-caché fuera de la zona protegida

- Proxy-caché en la DMZ2

Veamos cada una de las situaciones:

1. **Proxy-caché dentro de la zona protegida (proxy interno).**

   Se asume que el proxy es un host en el que se confía y además queda protegido por el propio cortafuego.

   Si el proxy comparte la caché con otros servidores habrá que configurarla como 'parent' ya que los cortafuegos suelen impedir el tráfico ICP por ser de tipo UDP.

2. **Proxy-caché fuera de la zona protegida (proxy externo).**

   Se asume que el proxy es un host en el que no se confía, no queda protegido por el propio cortafuego y está expuesto a posibles ataques.

   Un motivo para ubicar al servidor proxy de esta forma es para que pueda comunicarse por ICP con otros proxys.

   En este caso los navegadores deben configurarse para no utilizar el proxy para acceder a los servidores internos.

   En este caso también la caché no está protegida por el cortafuegos, por lo que su configuración es más delicada:

1. Sólo debe aceptar peticiones HTTP desde el cortafuegos para que usuarios no autorizados no puedan utilizar el proxy.
2. Al no confiar en dicha máquina debe colocarse en un puerto de un switch separado de otras máquinas.

3. Proxy-caché en la DMZ

Si la instalación dispone de red perimetral el proxy debe ser ubicado en la DMZ junto con los otros servidores de la organización.

Los navegadores de los clientes sí que podrán utilizar siempre el proxy.

El servidor caché acepta las peticiones desde el cortafuegos.

Deben permitirse conexiones entre la caché y los servidores web (80,443) y puede habilitarse el tráfico UDP para permitir comunicaciones por ICP.

Pensando en un aula de centro educativo lo usual es utilizar el propio servidor de aula como servidor proxy-caché. No es lo más seguro pero si lo más habitual.

3.1.9. ARCHIVOS DE LOGS

Squid genera los siguientes archivos de log:

- /**var/log/squid/access.log:** almacena las peticiones que se le hacen al proxy. De esa forma se puede conocer cuántos usuarios utilizan el proxy, cuáles son las páginas más visitadas. Mantiene una entrada por cada consulta HTTP con la IP del cliente, la URL pedida, etc. Existen aplicaciones que obtienen informes de este archivo de logs con el análisis de los datos almacenados. Por ejemplo Squid-Log_Analyzer.

TABLA III. IV. ARCHIVOS DE LOGS

Archivos/Directorios	Descripción
/var/log/squid/access.log	Archivo registro de peticiones al proxy.
/var/log/squid/cache.log	Archivo de accesos a la caché, errores, mensajes de inicio,... Relacionado con cache_log.
/var/log/squid/store.log	Histórico de la caché propiamente. Estado de los objetos almacenados en la caché. Páginas que se añaden, se quitan. Su información no es muy importante y se puede desactivar añadiendo la línea: cache_store_log none
/var/spool/squid/	Directorio caché. Relacionado con cache_dir.

Tabla III.IV. Ubicación de los archivos de registro

Se puede indicar en /etc/squid/squid.conf los paths en los que serán creados estos archivos:

```
cache_dir ufs /var/spool/squid 100 16 256

cache_access_log /var/log/squid/access.log

cache_log /var/log/squid/cache.log

cache_store_log /var/log/squid/store.log
```

En la primera línea indica donde quedará almacenada la caché y, el resto, los paths de los archivos de log.

Las páginas de error pueden mostrarse en diferentes idiomas. Para obtenerlas en español hay que establecer un enlace de la forma:

```
# ln -s /usr/share/squid/errors/Spanish /etc/squid/errors
```

En función del número de peticiones que reciba el proxy este archivo puede llegar a crecer a 1MB por minuto. Puede, por tanto, colapsar la partición.

Como este archivo aumenta de tamaño muy rápido, conviene hacer que se reinicie cada día. Si queremos guardar los registros de los 7 últimos días en el archivo /etc/squid/squid.conf establecemos una rotación de 7 con el parámetro logfile_rotate:

logfile_rotate 7

squid -k rotate

3.1.10. ARRANQUE DEL SERVICIO SQUID

Antes de arrancar Squid, y sólo la primera vez, habrá que ejecutar la orden siguiente para crear los directorios de la caché donde se guardarán las páginas.

squid –z

Para activar o desactivar el servicio:

/etc/rc.d/init.d/squid {start|stop|reload|force-reload|restart}

Si no se dispone de DNS hay que iniciar el servicio con la opción -D.

Una buena práctica consiste en incluir todas las modificaciones al archivo /etc/squid/squid.conf en el archivo /etc/squid/local-squid.conf. Este archivo local irá con un Include en el archivo general de configuración.

Después de hacer modificaciones en el archivo de configuración hay que relanzar el servicio. También se pueden activar las modificaciones, sin necesidad de parar el servicio, mediante la orden:

```
# squid -k reconfigure
```

Si queremos automatizar el arranque de Squid utilizamos la orden rcconf:

```
# rcconf squid
```

3.1.11. CONFIGURACIÓN DEL NAVEGADOR WEB

La mayoría de los navegadores permiten su configuración para trabajar a través de un proxy y dicha configuración es muy similar en todos ellos.

Estos navegadores deben ser configurados con el puerto e IP del servidor proxy.

Internet Explorer: Herramientas -> Opciones de Internet

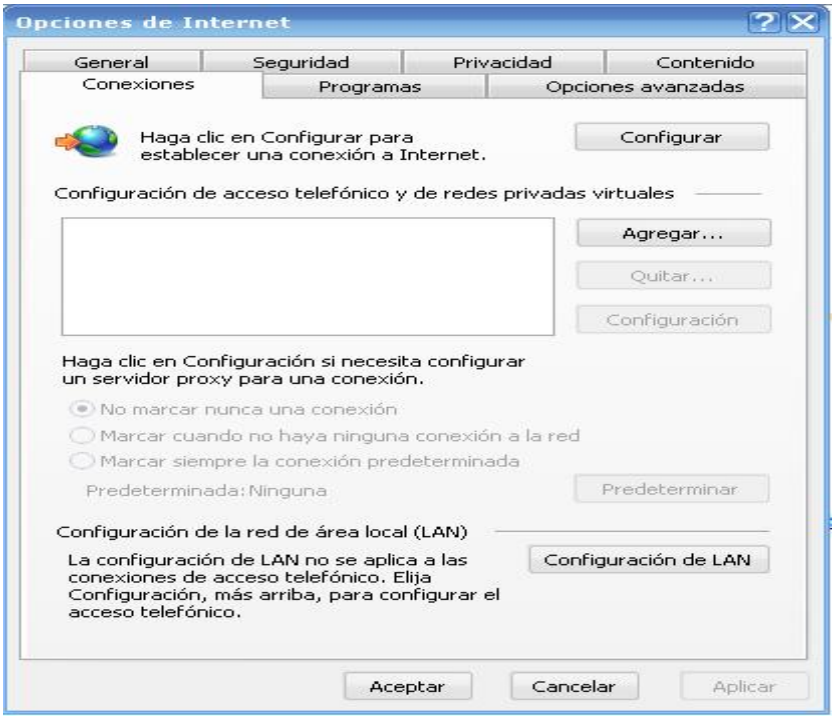


Figura III.16 Configuración del navegador

Conexiones -> Configuración de LAN (en servidor proxy introducir la IP del servidor Squid y el puerto).

Figura III.17. Configuración Lan

Firefox: Herramientas -> Opciones

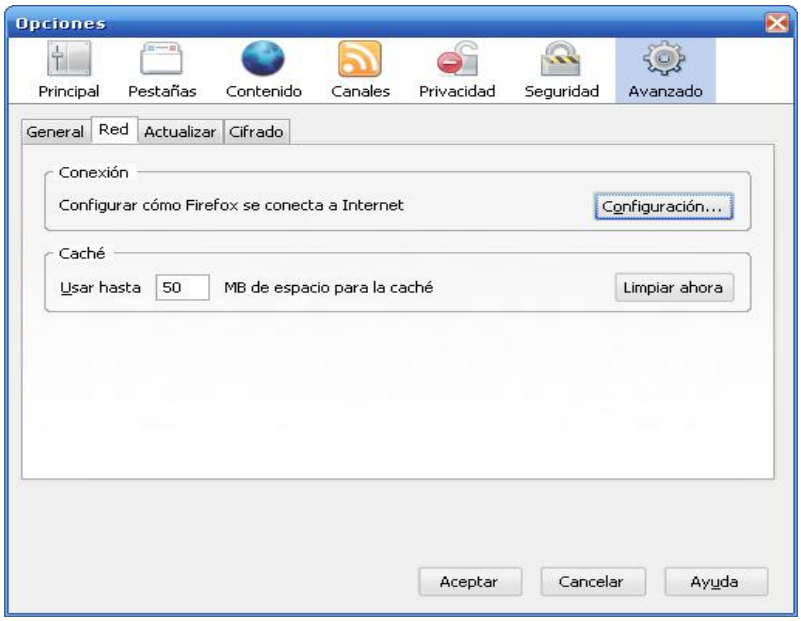


Figura III.18. Opciones de configuración

Configuración -> Configuración manual del proxy

Figura III.19. Configuración manual

3.1.12. ARCHIVOS DE AUTOCONFIGURACIÓN

Es posible también realizar la configuración de los clientes utilizando un archivo de configuración automática y de esa forma centralizar los cambios realizados. Este archivo se llama proxy.pac y es un script creado por el administrador del sistema.

Este script establece el modo con el que los navegadores web acceden a Internet y se guarda en una dirección a la que tienen acceso, en modo lectura, todos los clientes web. Normalmente se sitúa en un servidor web, como por ejemplo, Apache. Dicha dirección se tendrá que indicar al configurar el navegador.

La utilización de proxy.pac tiene la ventaja de que el administrador del sistema puede realizar cambios de forma transparente al usuario y sin necesidad de introducir modificaciones en los navegadores web. Por ejemplo, un cambio en la IP del proxy.

Incluimos el contenido de un archivo proxy.pac genérico para que sobre él se comprenda su estructura y funcionamiento.

```
function FindProxyForURL(url,host)

{ if (dnsDomainIs(host, "aula"))

return "DIRECT";

else if (isInNet(host, "10.0.2.0", "255.255.255.0"))

return "DIRECT";

else if (isInNet(host, "127.0.0.1", "255.255.255.255"))
```

return "DIRECT";

else return "PROXY proxy:3128"; }

El archivo contiene una función FindProxyURL que lleva como parámetros la URL a la que quiere acceder el navegador y la máquina que contiene el recurso.

Los bloques if-else indican que hay contenidos que están en el dominio 'aula' o en máquinas de la propia red local (10.0.2.0). El acceso, por tanto, es directo (DIRECT), sin intermediarios.

El resto de contenidos que no entran dentro de la estructura -if- se direccionan a través del proxy SQUID indicando PROXY máquina: puerto.

Este contenido se guarda en el archivo /var/www/proxy/proxy.pac y se le dan permisos 644 (rw - r - - r - -) y se deja disponible mediante un host virtual http://proxy o en la dirección http://10.0.2.254/proxy/proxy.pac.

Figura III.20. Ubicación de archivo proxy.pac

3.1.13. CONFIGURACIÓN DE SQUID PARA EL ACCESO A INTERNET POR AUTENTICACIÓN

Por defecto Squid se configura de forma que el usuario tiene acceso sin ningún tipo de autenticación.

Una forma de ampliar la seguridad con Squid es utilizar usuarios validados para controlar la conexión a Internet. Para ello vamos a suponer que existe un usuario 'profesor' con su correspondiente contraseña, que va a disponer de acceso total a Internet.

La lista ACL correspondiente a incluir será:

```
acl profesor_autorizado ident profesor
```

Se indica que el usuario de identidad 'profesor' dispone de una regla de control de acceso específica.

La regla de control de acceso correspondiente será:

```
http_access allow profesor_autorizado
```

Para controlar el acceso a Internet desde Squid se puede también utilizar el método de las autorizaciones (proxy_auth) que requiere de un procedimiento de validación de los usuarios para la utilización del Squid.

Un sistema de autenticación permite controlar quien va a poder conectarse a Internet independientemente de la máquina de la red local desde la que se haga la conexión. Como mecanismo de autenticación se utilizará ncsa_auth que viene incluido en Squid. Hay otros mecanismos de autenticación válidos como LDAP, SMB, PAM.

Para ello:

- Creamos el archivo squid_passwd en el que se almacenarán los logins de los usuarios junto con las contraseñas cifradas:

  ```
  # touch /etc/squid/squid_passwd
  ```

- y almacena en el archivo squid_passwd parejas de valores nombre_usuario: contraseña.
- Cedemos la propiedad del archivo al usuario 'proxy':

  ```
  # chown proxy:proxy /etc/squid/squid_passwd
  ```

- Sólo el usuario 'proxy' podrá leer y escribir en este archivo:

  ```
  # chmod 600 /etc/squid/squid_passwd
  ```

- Damos de alta a los usuarios:

```
# htpasswd /etc/squid/squid_passwd usuario1
```

- Introducimos la contraseña y confirmamos.

Estas cuentas son independientes de las del sistema o de cualquier otro servicio y sólo sirven para las conexiones a Internet a través del proxy Squid.

A nivel de archivo de configuración /etc/squid/squid.conf hay que incorporar una serie de parámetros necesarios:

- Indicar el programa de autenticación que va a ser utilizado (en nuestro caso ncsa_auth). Añadir la línea:

```
autenticate_program /usr/lib/squid/ncsa_auth /etc/squid/squid_passwd
```

- Se establece como lista de control de acceso la obligación de autenticarse ante Squid:

```
acl control proxy_auth REQUIRED
```

Ahora, siguiendo con el ejemplo de la red local con sólo ciertas IPs permitidas, la configuración deacl todo src 0.0.0.0/0.0.0.0

```
acl localhost src 127.0.0.1/255.255.255.255

acl aula src "/etc/squid/permitidos"

acl control proxy_auth REQUIRED
```

http_access allow localhost

http_access allow aula control

http_access deny todo Squid queda de la siguiente forma:

Por último, hay que relanzar el servicio:

/etc/rc.d/init.d/squid restart

3.1.14. CONFIGURACIÓN DE UN PROXY TRANSPARENTE

Hasta aquí hemos explicado el objetivo, configuración y funcionamiento de un proxy 'normal'. Hay ocasiones en las que no interesa que los usuarios sepan que están saliendo a Internet a través de un proxy, o se quiere forzar la utilización del proxy sin tener que estar configurando todos los navegadores disponibles en la red.

Esta es la misión del proxy transparente: interceptar todas las peticiones web de los clientes de forma transparente, de forma que los clientes creen estar saliendo directamente a Internet.

Sin embargo tiene el inconveniente de que no se puede hacer una autenticación del usuario por contraseña.

El proxy transparente utiliza el puerto 80 y el redireccionamiento de peticiones, por lo que no hay necesidad de modificar la configuración de los navegadores web para

utilizar el servidor proxy, será suficiente utilizar como puerta de enlace la IP del servidor. Como el servidor Apache utiliza el 80 será necesario configurar el servidor web para que utilice otro puerto de los disponibles.

Hay que tener el sistema de reenvío (forwarding) activado, que es el que permite a la máquina actuar como router. Ejecutar:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Las líneas siguientes de /etc/squid/squid.conf hay que dejarlas de la forma siguiente para que Squid reconozca el tráfico:

```
http_port 3128

httpd_accel_host virtual

httpd_accel_port 80

httpd_accel_with_proxy on
```

Para proxy transparente conviene dejar Squid en el puerto por defecto 3128.

Para el reenvío de las peticiones hay que incorporar una regla IPTABLES mediante la línea:

```
sbin/iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j
REDIRECT --to-port 3128
```

Cualquier petición que vaya al puerto 80 es redirigida a Squid, y no hay que modificar cada uno de los navegadores de los clientes. Aunque sólo sirve para peticiones HTTP.

3.1.15. CONCLUSIÓN

A lo largo del artículo se ha explicado la configuración básica del servicio Squid, así como los parámetros más importantes de su configuración, valores posibles y funcionalidades. Como se habrá podido observar las posibilidades de Squid son muy grandes y no se ha tocado nada del tema de monitorización del servicio e incluso su utilización como filtro de contenidos. Existen potentes herramientas para llevar a cabo estás funciones, como son Sarg o Squidguard.

Hemos utilizado la edición directa de los archivos de configuración y la ejecución de las órdenes relacionadas con su funcionamiento. Es una forma de conocer mejor los detalles de la configuración del servicio. Eso no quita la posibilidad de utilizar algún tipo de herramienta gráfica para su configuración, como puede ser Webmin y que puede ser tema de un artículo específico para esta herramienta.

1) Para un proxy transparente escuchando en el puerto 80 habría que modificar: httpd_accel_port 80 y añadir la línea: httpd_accel_uses_host_header on.

2) DMZ: En seguridad informática, una zona desmilitarizada (DMZ) o red perimetral es una red local (una subred) que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

3) Solo para esta sesión. Si se quiere de forma permanente hay que incluirlo en algún script rc de arranque.

3.2. PFSENSE

3.2.1. INTRODUCCIÓN A PFSENSE

Pfsense es una distribución basada en FreeBSD, para usarlo en servicios de redes LAN y WAN tales como firewall, enrutador, servidor de balanceo de carga, derivada de m0n0wall. Su objetivo es tener un cortafuego (firewall) fácilmente configurable a través de una interface web e instalable en cualquier PC, incluyendo los miniPC de una sola tarjeta. Es una solución muy completa, bajo licencia BSD y, de libre distribución.

De acuerdo al portal oficial de pfsense para el 2010 pfsense ha tenido más de un millón de descargas donde ha sido instalado con éxito en ambientes desde redes domésticas hasta grandes corporaciones. Pfsense cuenta con un gestor de paquetes desde su interfaz gráfica accedida remotamente para ampliar sus funcionalidades, al elegir el paquete deseado el sistema lo descarga y lo instala automáticamente. Existen 60 módulos disponibles para descargar al pfsense e instalarlos entre estos son el proxy squid IMinspector, Snort, ClamAV Pfsense puede ser instalado en cualquier ordenador PC o servidor independientemente de su arquitectura que cuente con un mínimo de 2 tarjetas de red.

El cortafuego forma parte del Kernel del sistema. Se trata del Packet Filter (PF) originario de OpenBSD, considerado como el sistema operativo más seguro del mundo.

Packet Filter (PF) está presente como estándar en FreeBSD desde noviembre de 2004. Incluye funcionalidades como el regulador de caudal ALTQ, que permite asignar prioridades por tipo de tráfico.

Los desarrolladores de pfSense escogieron FreeBSD en lugar de OpenBSD por su facilidad de instalación en el mundo de los PCs y porqué ya existía BSD Installer, una versión muy reducida de FreeBSD.

Todo ello da una gran flexibilidad a la solución pfSense, ya que se puede instalar tanto en equipos miniPC (basados en una sola placa) que emplean como disco una Compact Flash como en PC estándar con disco duro. En este último caso se pueden añadir paquetes como Snort, Squid, Radius, etc.

FREEBSD

FreeBSD es un avanzado sistema operativo para servidor moderno, el código base de FreeBSD ha sido objeto de más de treinta años de continuo desarrollo, mejora y optimización. FreeBSD es desarrollado y mantenido por un numeroso equipo de personas. Se dispone para redes avanzadas, con características de seguridad impresionantes, rendimiento de clase mundial y es utilizado por algunos de los sitios web más concurridos del mundo, redes integradas y dispositivos de almacenamiento.

MONOWALL

m0n0wall es un proyecto destinado a crear un paquete completo de software embebido servidor de seguridad que, cuando se utiliza junto con un computador integrado, proporciona todas las características importantes de las cajas de firewall comercial (incluyendo la facilidad de uso) a una fracción del precio (software libre). Está basado en una **versión de FreeBSD**, junto con un servidor web, **PHP** y otras utilidades de unos pocos. La configuración completa del sistema se almacena en un archivo XML de texto único para mantener las cosas transparentes. Es probablemente el primer sistema UNIX que tiene su tiempo de configuración de arranque realizado con PHP, en lugar de los scripts de Shell habituales, y que tiene la configuración completa del sistema se almacenan en formato XML

Su creador es Manuel Kasper que desde que comenzó a correr filtros de paquetes en ordenadores integrados, buscaba tener una interfaz, basada en web, amigable y que le permitiera controlar todos los aspectos de seguridad. Las soluciones existentes, tales como Webmin, no satisfacían sus necesidades, lo que lo indujo a escribir su propia interfaz.

LICENCIA BSD

La **licencia BSD** es la licencia de software otorgada principalmente para los sistemas BSD (*Berkeley Software Distribution*). Es una licencia de software libre permisiva

como la licencia de OpenSSL o la MIT License. Esta licencia tiene menos restricciones en comparación con otras como la GPL estando muy cercana al dominio público. La licencia BSD al contrario que la GPL permite el uso del código fuente en software no libre.

OPENBSD

El proyecto OpenBSD produce una multiplataforma **LIBRE** basada en 4.4BSD como sistema operativo UNIX. Nuestros esfuerzos por destacar la portabilidad, la normalización, la corrección, seguridad proactiva y criptografía integrada .

OpenBSD es de libre disposición de nuestros sitios FTP, y disponible también en un sistema barato de 3 CD. La versión actual es OpenBSD 4.8 que fue lanzado 01 de noviembre 2010.

OpenBSD es desarrollado enteramente por voluntarios. El proyecto paga por el entorno de desarrollo y los eventos para desarrolladores mediante la venta de CDs a través de una colección de tiendas y aceptando donaciones de organizaciones e individuos. Estas finanzas garantizan que OpenBSD siga existiendo y sea libre de usar para todos y la reutilización como mejor les parezca, camisetas y carteles están disponibles también, pero no financiar el proyecto.

3.2.2. FUNCIONALIDADES

Pfsense es una aplicación que se instala como un sistema operativo ya que tiene varias funcionalidades entre estos servicios de redes LAN y WAN, con detalle estos servicios son los siguientes:

FIREWALL: Pfsense se puede configurar como un cortafuego permitiendo y denegando determinado tráfico de redes tanto entrante como saliente a partir de una dirección ya sea de red o de host de origen y de destino, también haciendo filtrado avanzado de paquetes por protocolo y puerto.

SERVIDOR VPN: Pfsense se puede configurar como un servidor VPN usando protocolos de tunneling tales como IPSec, PPTP, entre otras.

SERVIDOR DE BALANCEO DE CARGA: Pfsense puede ser configurado como servidor de balanceo de carga tanto entrante como saliente, esta característica es usada comúnmente en servidores web, de correo, de DNS. También para proveer estabilidad y redundancia en él envió de tráfico a través del enlace WAN evitando los cuellos de botella.

PORTAL CAUTIVO: Este servicio consiste en forzar la autenticación de usuarios redirigiéndolos a una página especial de autenticación y/o para aceptar los términos de uso, realizar un pago etc. para poder tener acceso a la red. El portal cautivo es usado comúnmente para control de accesos a la red en los puntos de accesos inalámbricos de los hoteles, restaurantes, parques y kioscos.

TABLA DE ESTADO: PFSense es un stateful firewall, el cual como característica principal guarda el estado de las conexiones abiertas en una tabla. La mayoría de los firewall no tienen la capacidad de controlar con precisión la tabla de estado. Pfsense tiene un enorme número de características que permiten una granularidad muy fina para el manejo de la tabla de estado.

SERVIDOR DNS Y REENVIADOR DE CACHE DNS: Pfsense se puede configurar como un servidor DNS primario y reenviador de consultas de DNS.

SERVIDOR DHCP: También funciona como servidor de DHCP, se puede también implementar VLAN desde Pfsense.

SERVIDOR PPPOE: Este servicio es usado por los ISP para la autenticación de usuarios que puedan ingresar a internet, por una base local o vía radius.

ENRUTAMIENTO ESTÁTICO: Pfsense funciona como un enrutador ya que entrega direccionamiento IP y hace el mateo hacia afuera.

REDUNDANCIA: Pfsense permite configurar dos o más cortafuegos a través del protocolo CARP (Common Address Redundancy Protocol) por si uno de los cortafuegos se cae el otro se declara como cortafuegos primario.

REPORTES Y MONITOREO: A través de los gráficos RDD Pfsense muestra el estado de los siguientes componentes:

- Utilización de CPU,
- Rendimiento Total.
- Estado del Firewall,
- Rendimiento individual por cada interface,
- Paquetes enviados y recibidos por cada interface,
- Manejo de tráfico y ancho de banda.

3.2.3. REQUISITOS

3.2.3.1. HARDWARE

Para la instalación de pfsense sobre arquitectura i386 los requerimientos de hardware son los siguientes.

1. Procesador Intel Pentium III, hasta un Intel Xeon, nada de AMD.

2. Memoria RAM desde 128 Mb hasta 3 Gb.

3. Disco Duro de 2 Gb hasta 80 Gb, IDE, SCSI, SATA Y SAS-SATA.

4. Dos Tarjetas de red cableadas Intel y Realtek (la red inalámbrica solamente funcionan las tarjetas de red marca Atheros).

5. El PC o servidor necesitará un teclado, monitor y opcionalmente un mouse, debido a que este servidor será administrado remotamente.

3.2.3.2. SOFTWARE

El software será instalado sobre un servidor o PC dedicado única y exclusivamente,

- Descargar de la pagina, la imagen a quemar de pfsense, esta viene comprimida "pfSense-1.0.1-LiveCD-Installer.iso.gz" luego de bajarla se puede usar la aplicación preferida para descomprimirla (winrar u otros).

3.2.4. INSTALACION DE PFSENSE

El proceso de instalación del pfsense se realiza de la siguiente manera:

Iniciar el computador que tiene dispuesto para instalar pfsense, esta es una versión LiveCD que puede ser usada desde una unidad CD-rom o DVD, al presentar la pantalla:

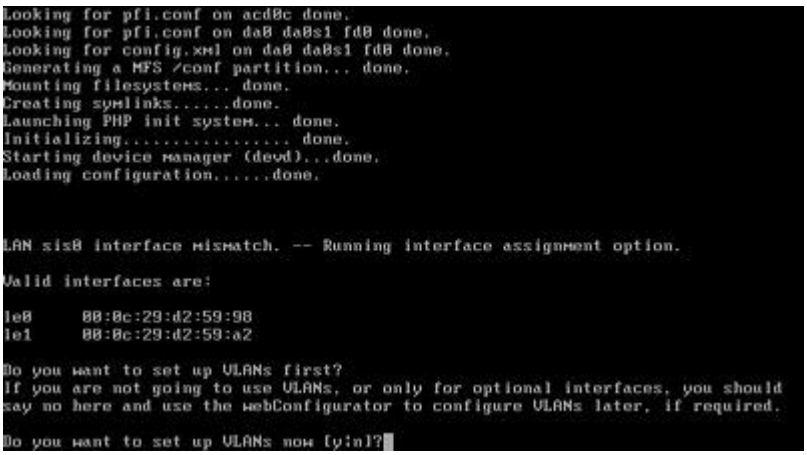


Figura III.21. Configuración de Vlan

- Indicar que no deseamos una Vlan y luego identificar cuáles serán las interfaces lan y wan

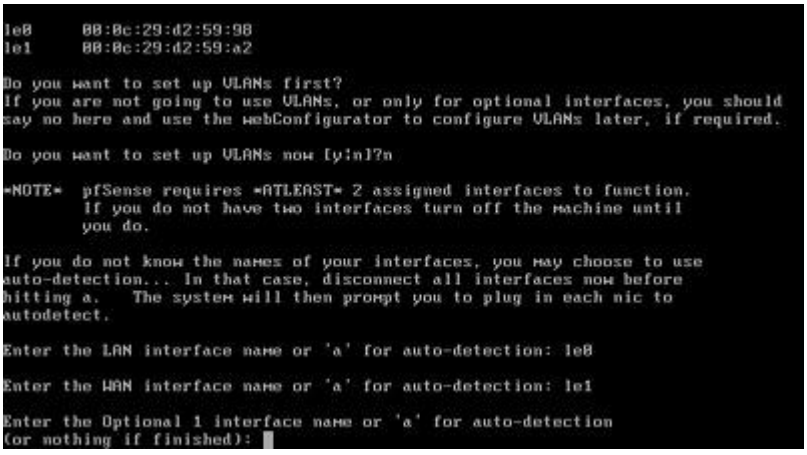


Figura III.22. Configuración de interfaces

- Seleccionada cuales serán las interfaces lan y wan, presionar enter para continuar, en este paso nos indicará si deseamos proceder con la selección, le indicamos que si,

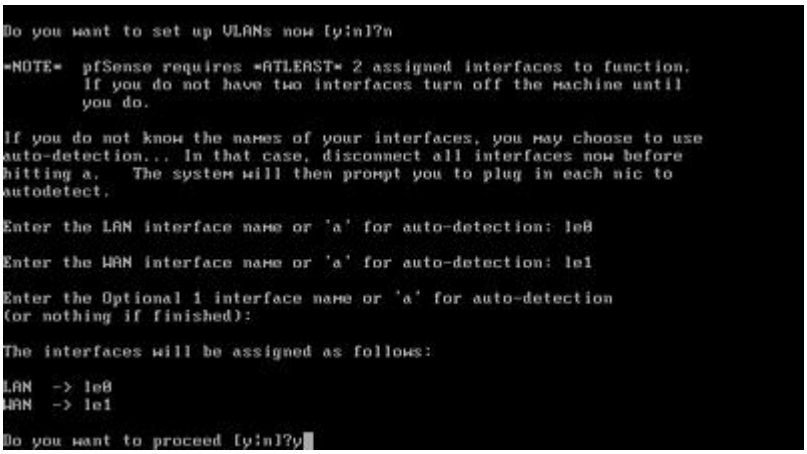


Figura III.23. Configuración seguir con proceso

- Luego del proceso que tarda unos minutos (pocos) se muestra el menú donde se escoge la opción 99

Figura III.24. Configuración Menú de Pfsense

- Esto inicia la instalación, se muestra un asistente, lo primero es el vídeo, aceptar por defecto.

Figura III.25. Configuración selección de vídeo

- En la siguiente pantalla seleccione la opción de la instalación de pfsense

Figura III.26. Configuración selección de Instalación de Pfsense

- Se indica un proceso para dar formato al disco duro, particionado, y copia de archivos.

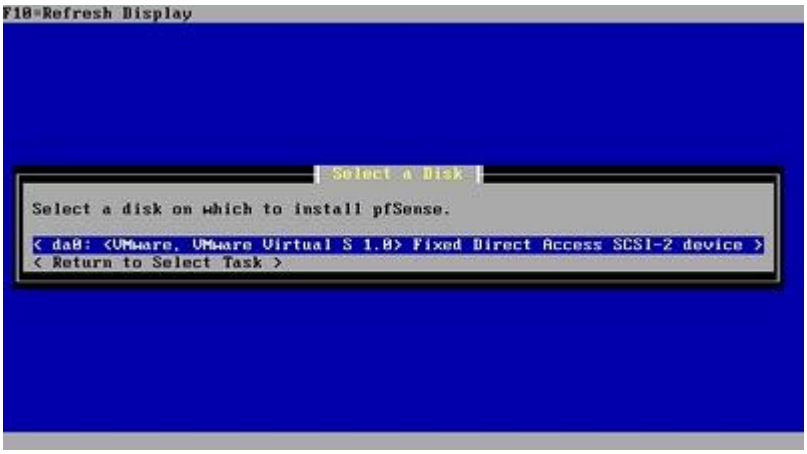


Figura III.27. Configuración selección de disco para dar formato.

- Presionar enter sobre el disco duro y le damos un primer formato al disco (esto borrará todo el contenido del disco)

Figura III.28. Configuración formato de disco

- Por lo general la geometría del disco duro es la correcta, así que seleccionar "usar esta geometría".

Figura III.29. Configuración selección de geometría del disco

- Dar inicio a formato del disco.

Figura III.30. Configuración formato de disco en proceso

- Luego nos solicitará particionar el disco, esto es para instalar el sistema operativo FreeBSD.

Figura III.31. Configuración selección de partición de disco.

- Aunque por defecto esta marcado FreeBSD se puede seleccionar otros sistemas de archivos, no es necesario ya que estamos usando FreeBSD :-D

Figura III.32. Configuración selección de FreeBSD para partición.

- Ahora se va a instalar el sector de inicio en el disco duro, debemos presionar enter en aceptar e instalar Bootblock

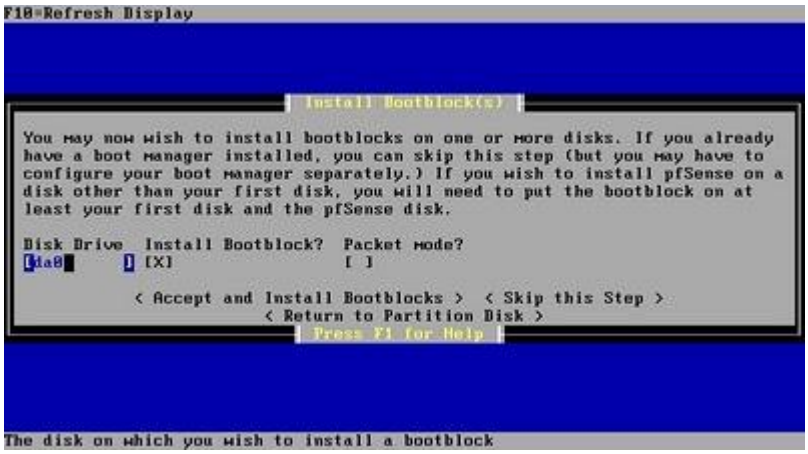


Figura III.33. Configuración instalación del sector de inicio.

- Nos preguntará en que partición vamos a instalar.

Figura III.34. Configuración selección de partición primaria.

- En el ejemplo usamos un disco pequeño (811 MB) utilizar la opción por defecto, es decir dos particiones una para el archivo de intercambio y otra para la raíz "/", el asterisco en Capacity solo indica que tomará todo el espacio disponible en el disco

Figura III.35. Configuración selección de sub partición

- Luego de otras pantallas, si aparece la siguiente es porque ya se están copiando los archivos al disco, esto tarda unos 7 minutos (pentium II con 128 de ram)

Figura III.36. Configuración progreso de copia de archivos

- Luego de esto pedirá reiniciar la máquina.

Figura III.37. Configuración selección de reinicio de máquina

- Por defecto la interfaces lan utiliza la dirección ip 192.168.1.1 ya que pfsense está por defecto para dar servicio de NAT, se debe cambiar la ip de la máquina a 192.168.1.x para así poder acceder y configurar vía interface lan.

3.2.5. CONFIGURACIÓN

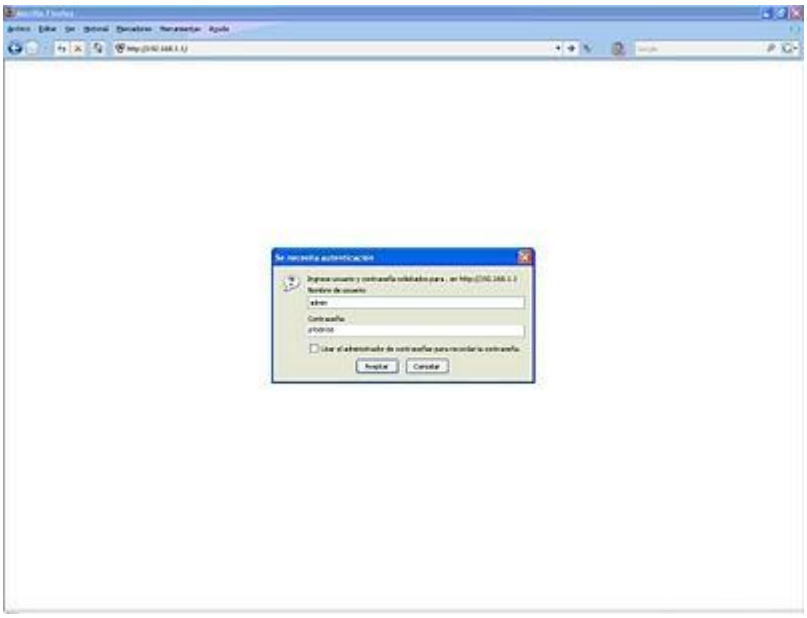


Figura III.38. Validación de usuario y contraseña

La primera pantalla que se verá vía web, es la solicitud de usuario y contraseña, esta por defecto para el user es admin y el password es pfsense, en la próxima pantalla ya estará dentro de entorno web de pfsense.

1. Seleccionar **interfaces > wan**, allí aparece esta pantalla donde seleccionaremos static añadimos la ip y puerta de enlace (de nuestra red), desplazando la página hacia abajo también desmarcaremos: Block private networks. Una vez aceptados los cambios deberemos conectarnos vía web por la interfaz wan (antes ya debemos cambiar la ip de nuestra estación de trabajo a la red con la que realmente estamos trabajando en este ejemplo sería una ip 192.168.10.xxx y no una ip 192.168.1.xxx

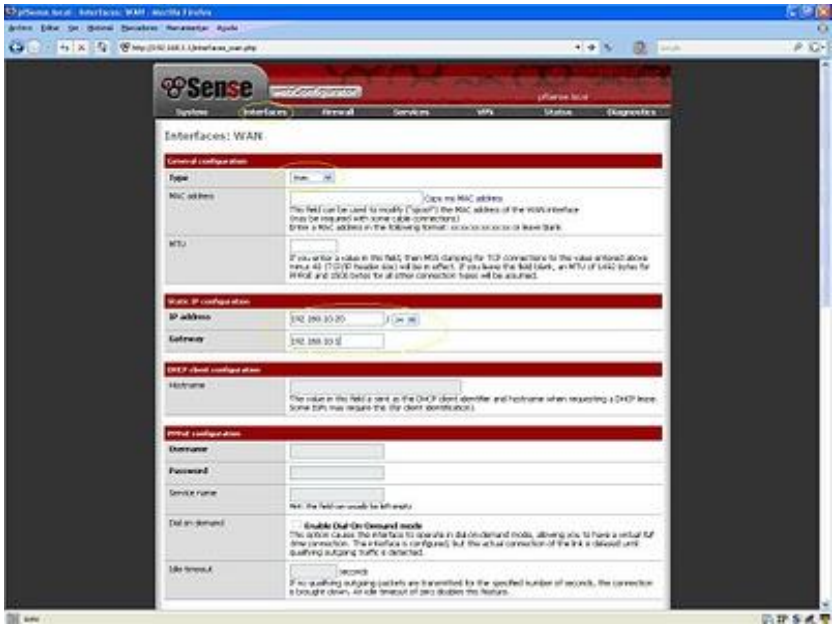


Figura III.39. Configuración interfaz Wan

2. En **interfaces > lan,** encojemos en la opción Bridge with la interfaz wan, y colocamos la misma ip que añadimos a la interfaz wan, además de marcar la opcion FTP Helper (Disable the userland FTP-Proxy application),

Figura III.40. Configuración interfaz Lan

3. Aceptando los cambios ahora nos vamos a system > Advanced

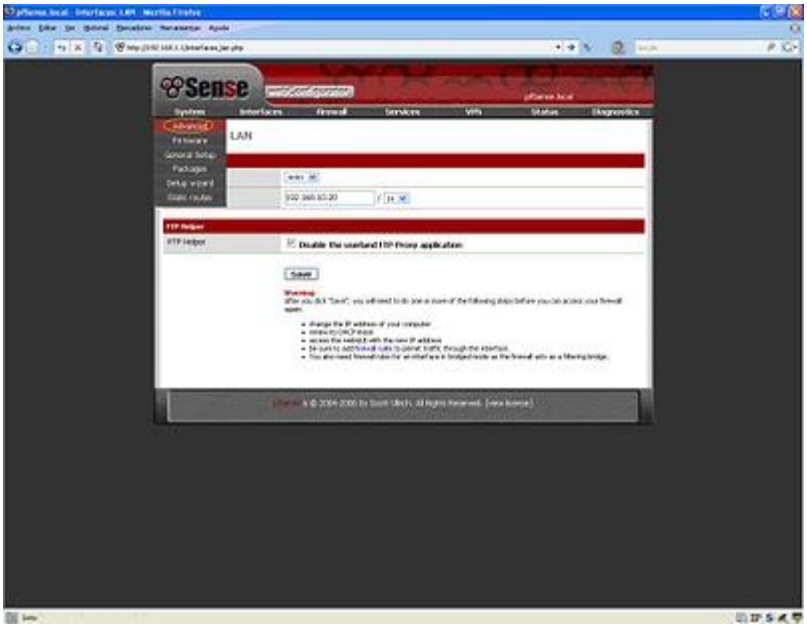


Figura III.41. Configuración System\Advanced

4. En Advanced buscaremos filtering bridge y la activaremos, también se puede activar otras opciones como Secure shell pasa acceder por ssh.

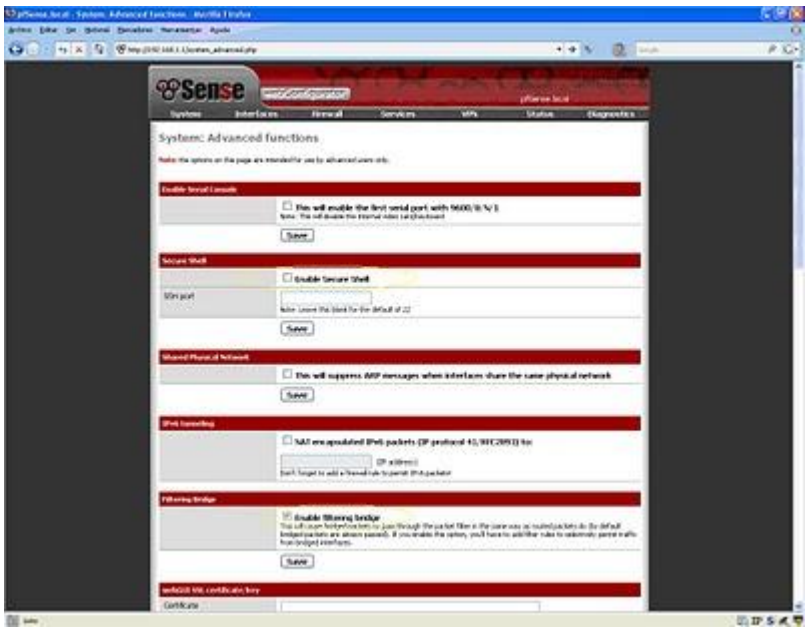


Figura III.42. Configuración Secure Shell

5. Ahora nos vamos a System > General Setup,

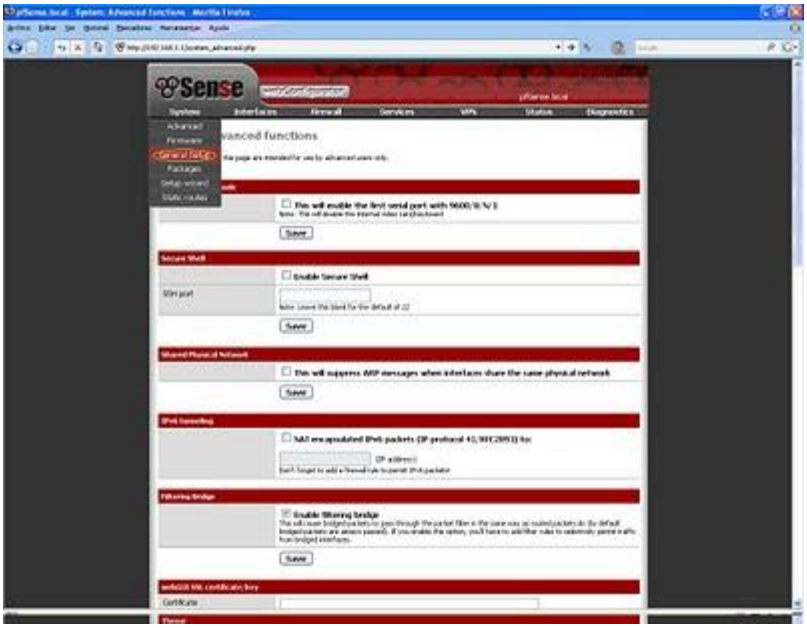


Figura III.43. Configuración System\General Setup

6. Aquí se puede cambiar el hostname, domain, añadimos los Dns de nuestro ISP, y desmarcamos allow DNS server list to be overridden by dhcp/PPP on WAN. Guardamos los cambios.

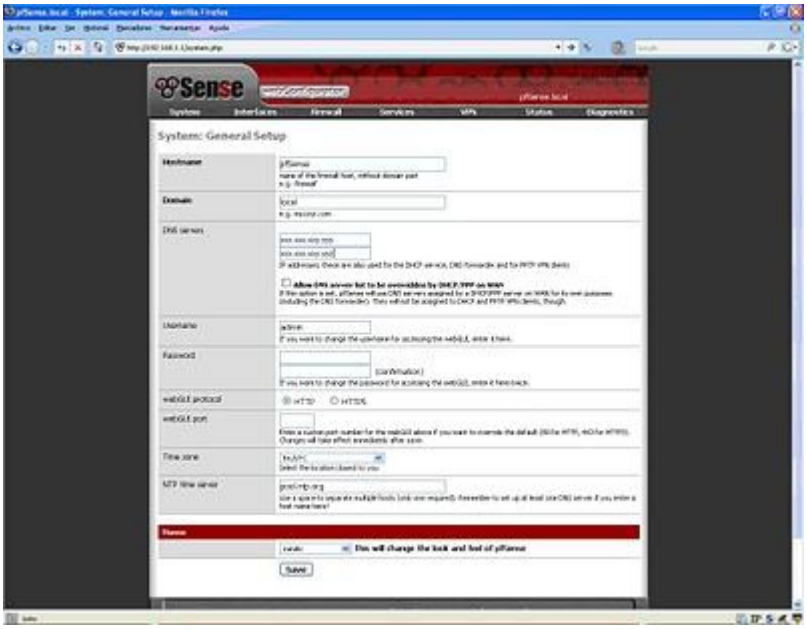


Figura III.44. Configuración de parámetros generales del Setup

7. Ahora seleccionamos Firewall > NAT, allí debemos seleccionar Enable advanced outbound NAT

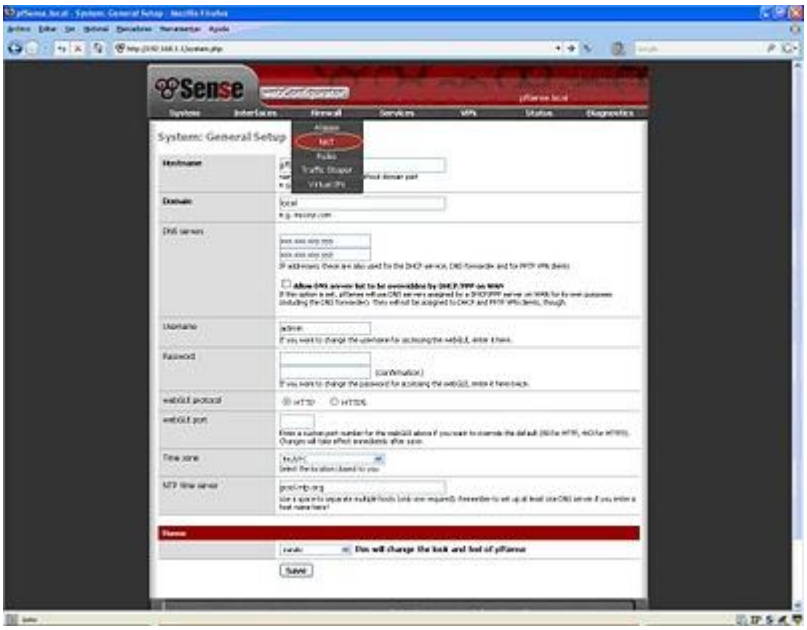


Figura III.45. Configuración de Firewall \Nat

8. Se debe borrar todas la reglas que aparecen en la lista, esto es importante porque si no se hace el Firewall Transparente que queremos no funcionará, recuerde aplicar los cambios en todo momento de la configuración, si ya tiene un servidor dhcp en tu red lan, debe desactivar el que trae pfsense, lo encontrará en Services> dhcp, así no entrarán en conflictos las máquinas con ips duplicadas.

Existen otros servicios como DNS, en Diagnostics tiene una opción para respaldar toda la configuración que acaba de realizar si por algún motivo tiene que generar de nuevo el pfsense le ahorra mucho trabajo.

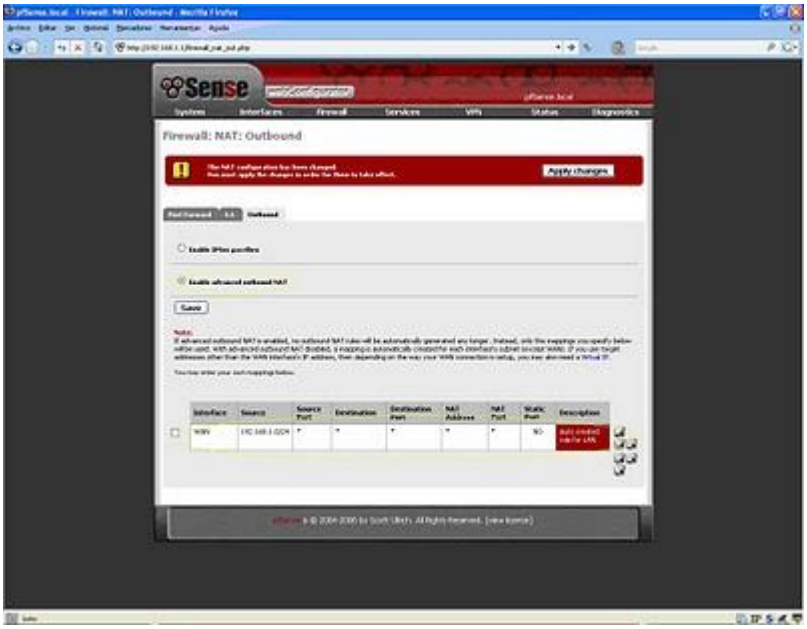


Figura III.46. Configuración parámetros de Firewall \Nat

9. Vamos a Firewall > rules, como se ve en la pestaña WAN no tiene ninguna regla, allí solo configurará reglas para DMZ y algunas conexiones entrantes.

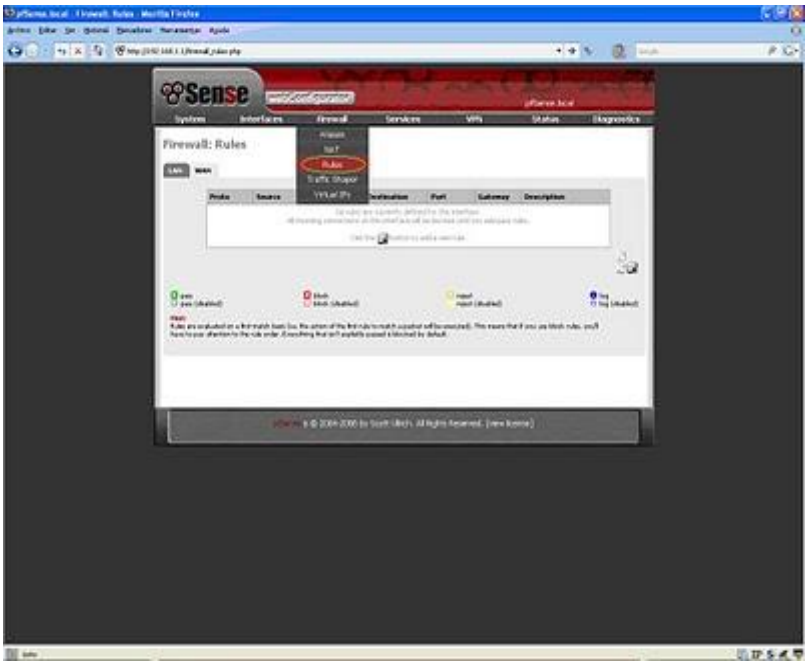


Figura III.47. Configuración de Firewall \Rules

10. Haciendo clic sobre la pestaña LAN veremos que la regla por defecto es permitir todo el trafico de la red lan, en este caso la editaremos y la desactivamos, pero primero añadiremos el tráfico que queremos dejar pasar (por defecto todo el trafico estará bloqueado), servicios tales como HTTP, HTTPS, SMTP, POP3, IMAP entre otros.

Figura III.48. Configuración parámetros de Firewall \Rules

11. Una vez añadido el conjunto de reglas que deseamos dejar pasar hacia internet, procedemos a editar la regla por defecto y la desactivamos, una vez aplicado los cambios esta se tornará atenuada con respecto a las otras.

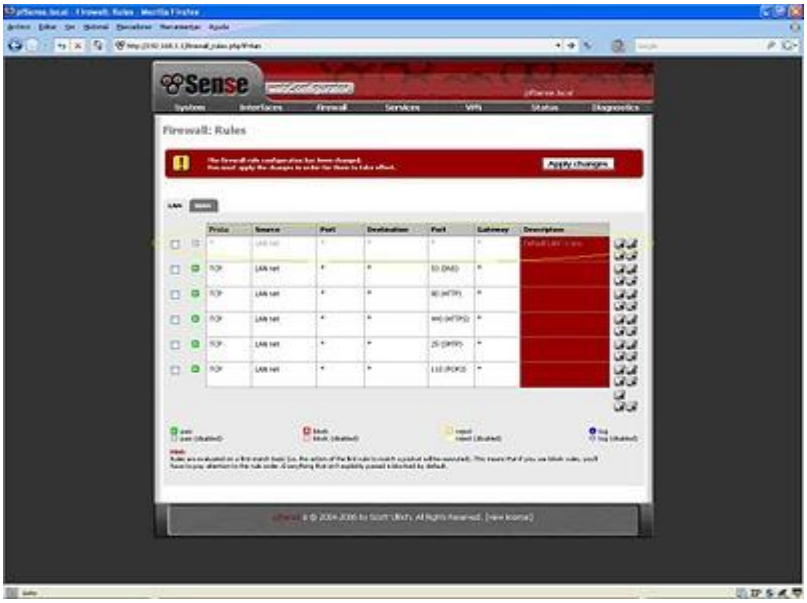


Figura III.49. Configuración edición de reglas

12 En la interfaz WAN podremos configurar que desde afuera acceden a un servidor web en este caso, donde 190.0.0.0 es nuestro servidor web de ejemplo

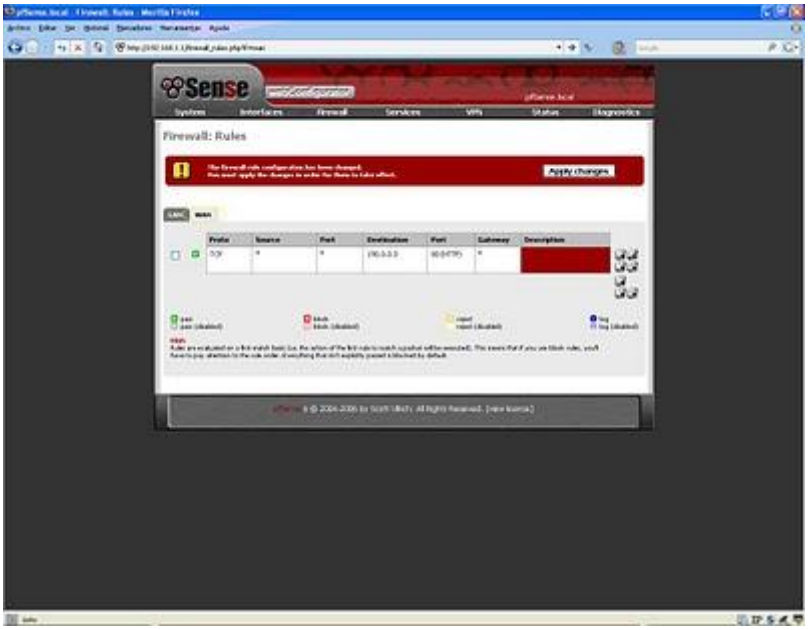


Figura III.50. Configuración edición de reglas en interfaz Wan

13. Como punto final en ***System > Packages*** podremos añadir paquetes adicionales como ntop, entre otros.

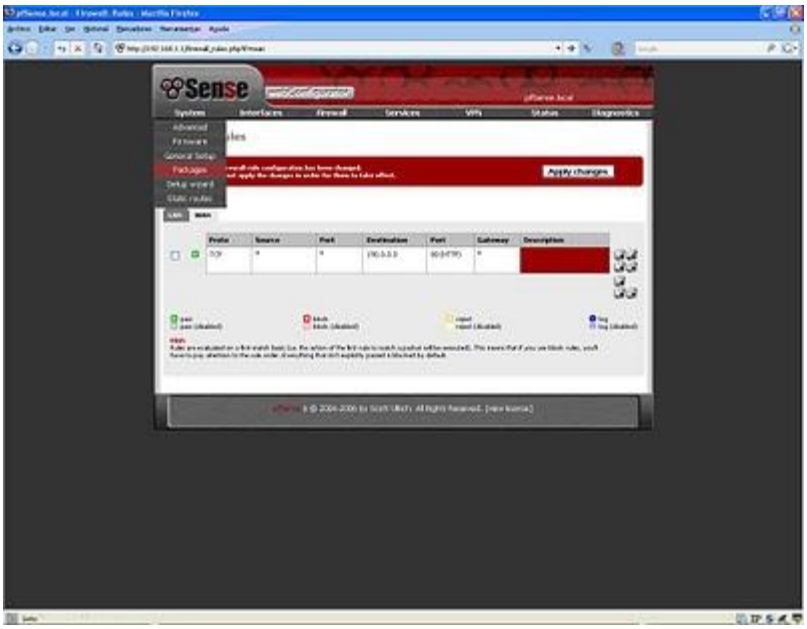


Figura III.51. Configuración System\Packages

14. Con estos pasos algo extensos se configura un Firewall Transparente. Proceso similar se debe seguir para instalar Squid, SquidGard y otros paquetes que incluye la herramienta.

CAPITULO IV

IMPLEMENTACIÓN DE UNA TÉCNICA DE CONTROL DE ACCESO A INTERNET Y SU APLICACIÓN EN LA RED DE DATOS EN EL COLEGIO "CORINA PARRAL"

4.1. INTRODUCCIÓN

El presente capitulo muestra la configuración de un servidor proxy y los pasos necesarios para la implementación del firewall y filtrado de paquetes para el laboratorio que cuenta con el servicio de internet otorgado de forma gratuita por el gobierno central para instituciones educativas.

Consciente de que una de las múltiples necesidades con las que cuenta el centro educativo es el control al acceso a internet, se realizo el estudio e investigación necesaria sobre las técnicas de control de acceso a Internet y luego de un análisis minucioso y comparación de la técnica más adecuada se procede a su implementación, con el fin de brindar seguridad y protección a la información de cada equipo de trabajo,

además se controla el acceso a información indebida durante el proceso de enseñanza aprendizaje en el laboratorio de práctica de los estudiantes del plantel.

El estudio de las diferentes técnicas me permitió determinar que a nivel de software existen diferentes aplicaciones que muestran excelentes prestaciones de seguridad y facilidad de uso y que se pueden instalar en el computador que sirve de servidor, para varios sistemas operativos de distribución libre y otras que requieren del pago de licencia para su utilización. De igual forma en lo referente a hardware se puede colocar equipo básico o sofisticado para controlar el acceso a la información que ofrece internet. Sin embargo por la forma de instalar, paquetes incluidos en la herramienta, configuración desde un entorno gráfico antes que de línea de comando o edición de reglas desde una archivo tipo texto, se selecciono e instalo la herramienta Pfsense 2.0, misma que se puede utilizar en una red pequeña (2-10 usuarios) hasta una grande (50-150 usuarios); en el laboratorio que se implementó tiene 18 máquinas que forman parte de una red inalámbrica.

Indicando además que en la actualidad el plantel educativo carece de servidor o implementación similar que permita controlar el acceso a la información que ofrece internet.

4.2. INSTALACIÓN DE PFSENSE

El proceso de instalación del pfsense se realizó de la siguiente manera:

- Se inició el computador desde la unidad de CD verificando arranque tal y como se muestra en esta pantalla.

Figura IV.52. Pantalla de Bienvenida a Pfsense

- A la pregunta si se necesita configurar VLAN [Y:N], señalamos que no luego pulsando la letra “a” indicando que detecte de forma automática las interfaces lan y wan

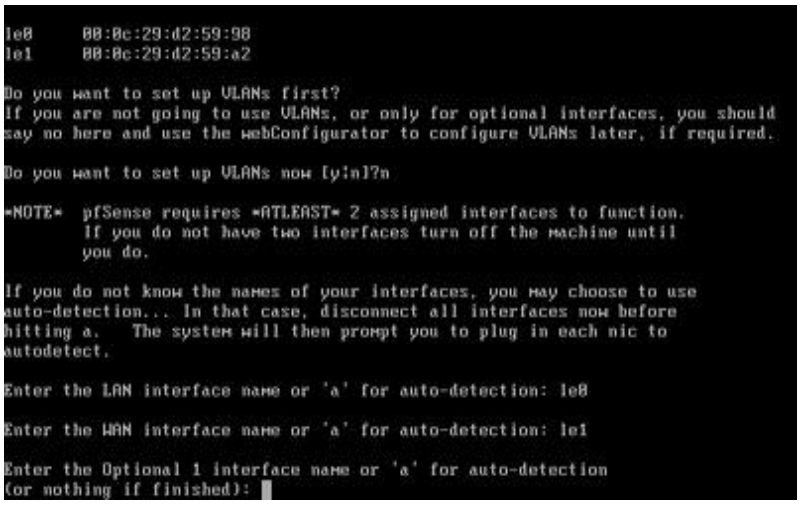


Figura IV.53. Configurar Vlans

- Luego de configurar el identificador de las tarjetas de red el sistema nos preguntara si esta configuración es correcta para proceder con la carga de archivos de instalación del pfsense donde pulsamos "Y". Nuestras interfaces son:

  WAN (wan): rl0 192.168.100.1

  LAN (lan): re0 192.168.1.1

  Algunas de las abreviaturas que se encuentran adelante de las MACS address son le0, em0; en el caso de las de realteck serán rl0, rl1 y así las identificaremos por el chipset que contienen

- Luego del proceso que tarda unos pocos minutos se muestra el menú con 16 opciones de configuración, se escoge la opción 99, para instalar Pfsense en disco duro de equipo seleccionado.

Figura IV.54. Menú de configuración de Pfsense

- Saldrá la siguiente pantalla. En esta pantalla seleccionaremos la opción “Accept these settings”. Se empezará a formatear el disco duro y copiar los archivos del sistema.

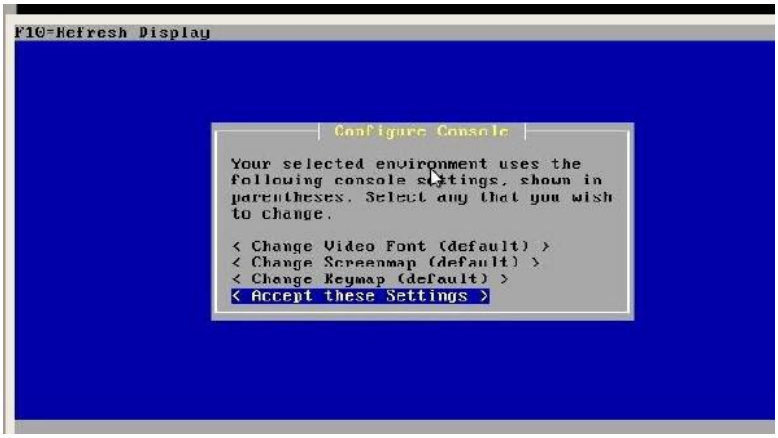


Figura IV.55. Menú de configuración de Consola

- La siguiente pantalla nos preguntará el tipo de instalación que deseamos aplicar a nuestro servidor, o si queremos recuperar el archivo de config.xml. Seleccionamos la opción Quick/Easy install.

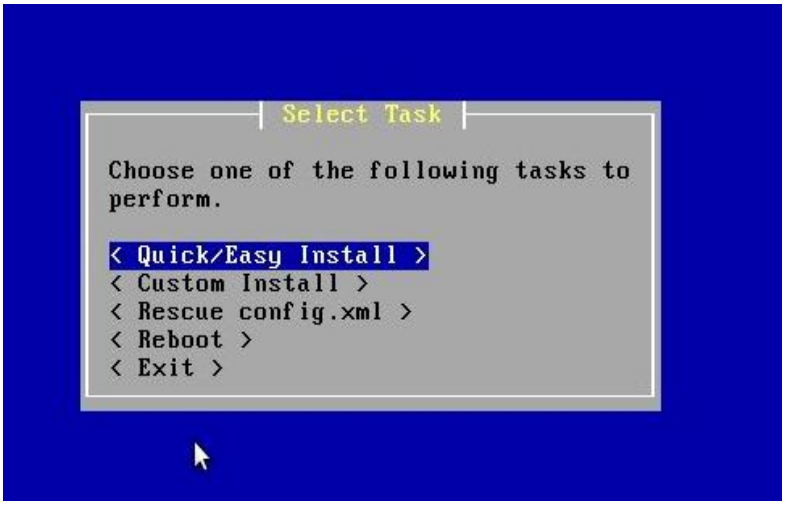


Figura IV.56. Menú de Selección de tarea de instalación

- Seleccionar el kernel para el procesador que estemos utilizando, en la mayoría de casos "uniprocessor kernel" las otras opciones se reservan para otros usos como programadores, o dispositivos que se manejan vía cable Serial.

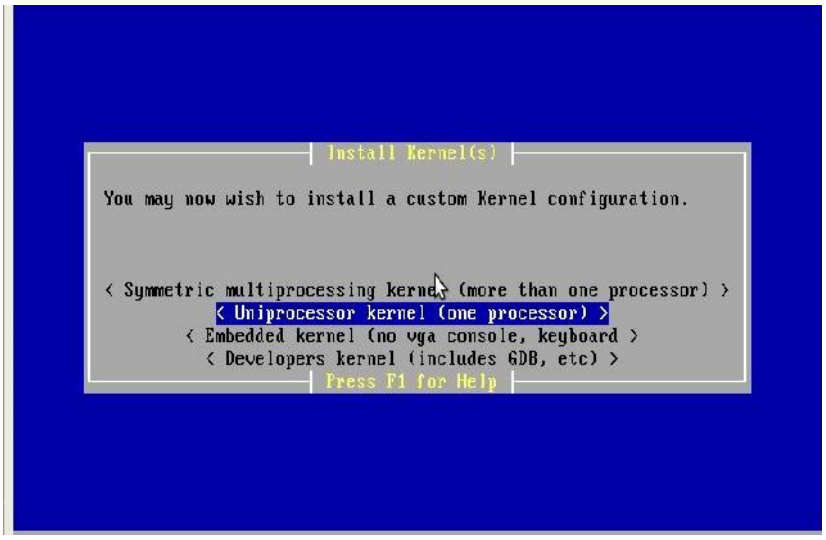


Figura IV.57. Menú de Selección del Kernel para el procesador

- Seleccionamos OK para dar por terminado el proceso de instalación del pfsense en el servidor dedicado.

Figura IV.58. Asegura proceso de instalación con OK.

- Para finalizar seleccionar “reboot”

Figura IV.59. Finaliza proceso de instalación con Reboot.

- Antes de reiniciar por HDD saldrá esta pantalla con el usuario y contraseña de ingreso a la consola web.

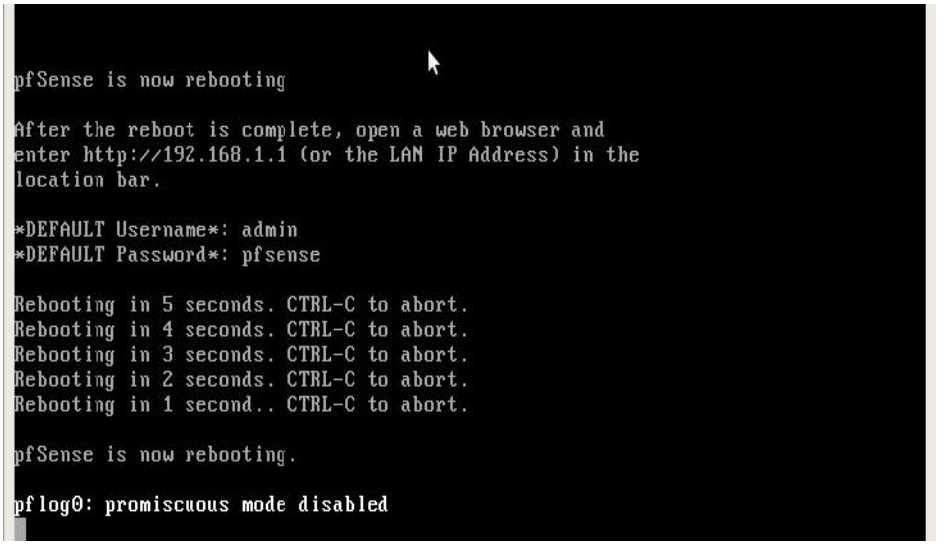


Figura IV.60. Usuario y contraseña para ingresar desde la consola web.

- Se inicia el servidor dedicado desde disco duro.

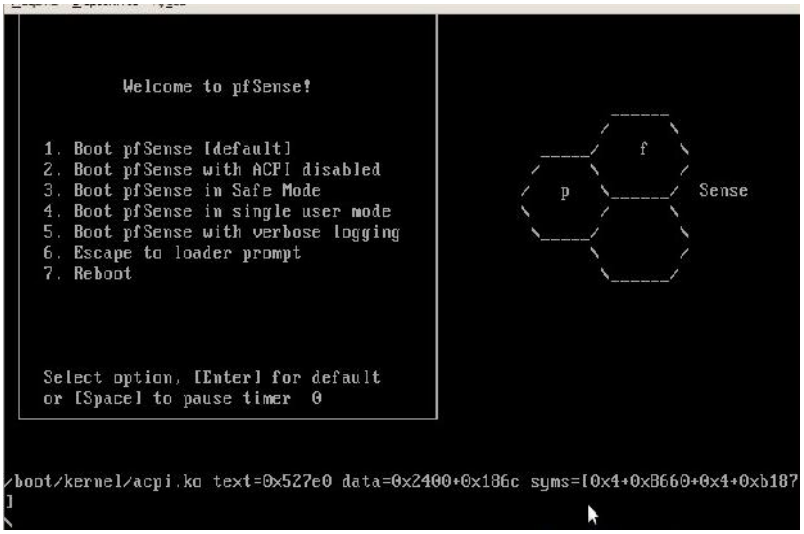


Figura IV.61. Inicio de Pfsense desde equipo.

- Comprobamos desde el servidor el acceso a internet del pfsense a través de un ping a una página web ejemplo http://www.google.com/ esto se hace con la opción 7.

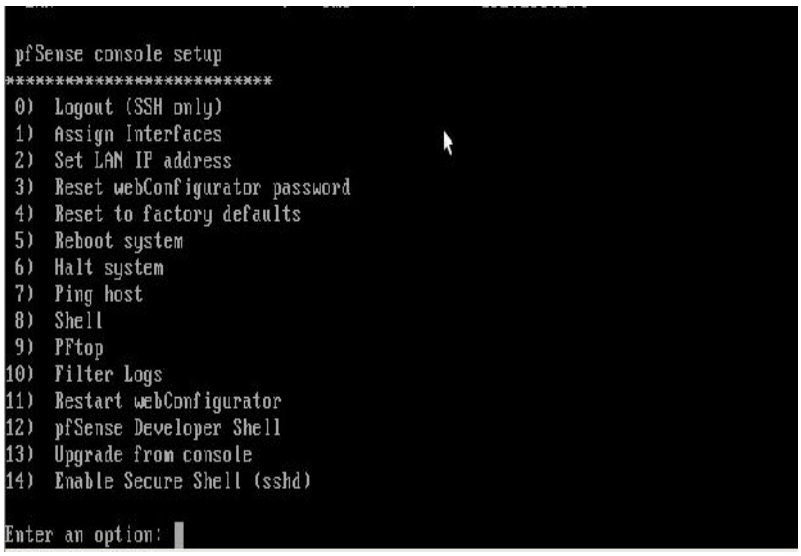


Figura IV.62. Verificación de acceso a internet con opción 7.

- Comprobamos que si tenemos conexión a internet.

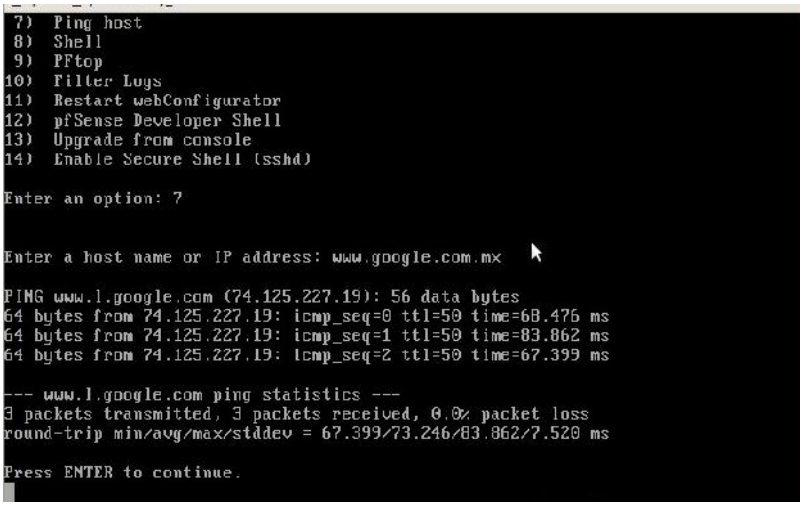


Figura IV.63. Respuesta de conexión.

- Para asignar otras direcciones IPs a la LAN se selecciona la opción dos y previa planeación utilice la siguiente configuración para la IP de la local:

IP: 192.168.2.0/24

mascara de subred: 255.255.255.0 /24

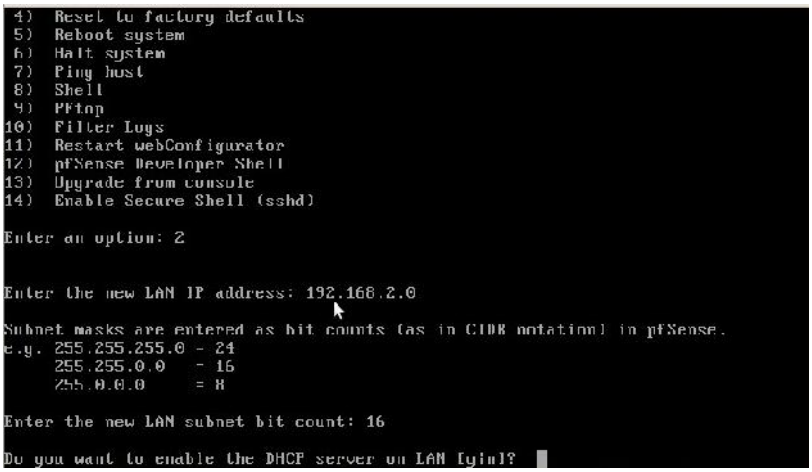


Figura IV.64. Asignación de direcciones IPs para LAN.

- También se habilitó el servicio DHCP, configurando la IP inicial y final.

  Ip inicial: 192.168.2.11

  Ip final: 192.168.2.50

- En la red lan desde un equipo diferente con sistema operativo windows o Linux se verificó que este tenga una ip entregada del servidor pfsense para poder acceder a la consola web. También se observa si tiene acceso a internet.

Figura IV.65. Acceso a internet en equipo diferente del instalado.

- Para ingresar a la consola web ingresamos la IP que configuramos previamente para la interfaz LAN http://192.168.2.1/ ; esta IP es la puerta de enlace que será entregada a los equipos cliente a través de DHCP.

Figura IV.66. Ingreso desde la consola web.

- A continuación en el asistente de configuración muy sencillo: Se estableció el nombre del host del proxy, nombre del dominio y las ips de los servidores DNS, esto si contamos con ips fijas. También se cambia en ***system > General Setup***.

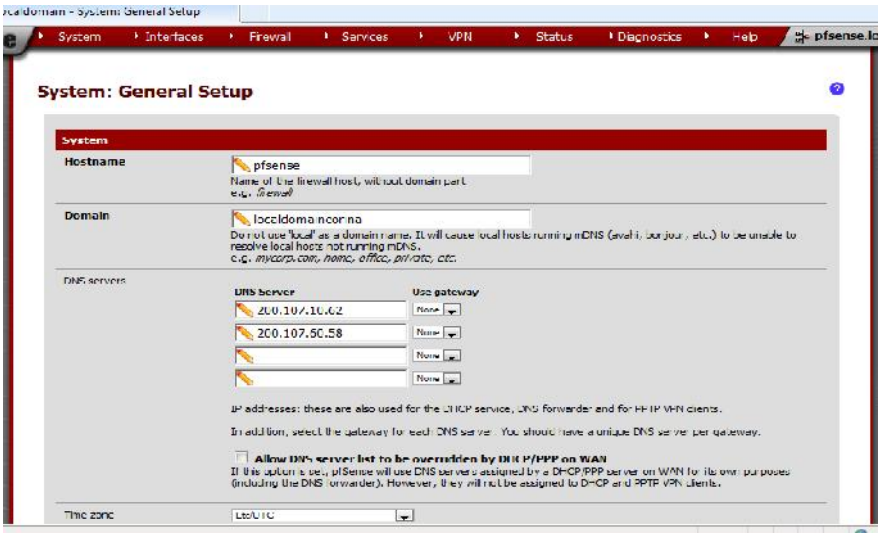


Figura IV.67. Asistente de configuración.

- Para la red WAN, seleccionar en Interfaces/WAN, esta por DHCP, esta configuración se toca cuando tenemos IPS fijas, el proveedor de servicios dedicados debe proporcionar los datos, como servidores DNS, puerta de enlace.

Figura IV.68. Configuración de interfaz Wan.

- Configurar el servidor de hora, es importante ya que AWStats funciona con él, y algunos servicios, útil sobre todo los que utilizan tareas programadas y reportes.

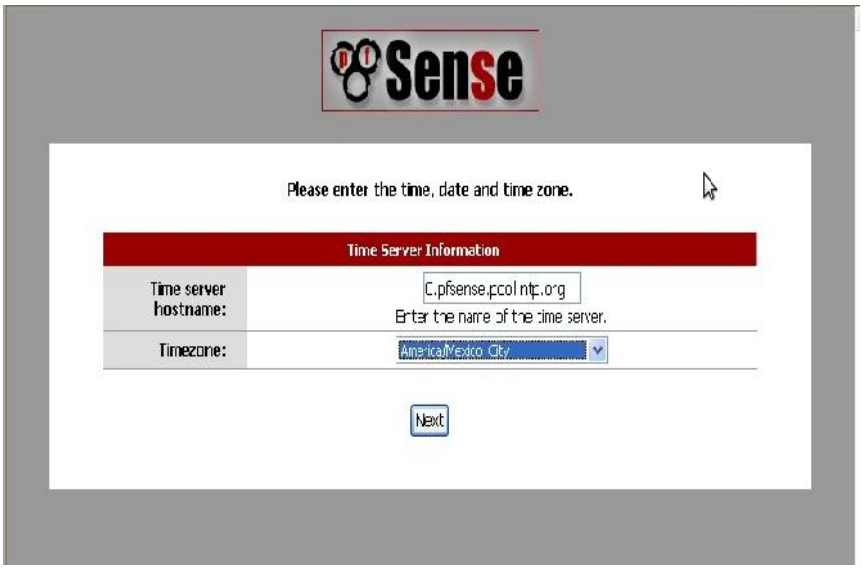


Figura IV.69. Configuración del tiempo del servidor.

- Para configurar la red LAN, Seleccione en Interfaces opción LAN y verificamos en Type: Static e IP Configuration: 192.168.2.1; dejar como esta.

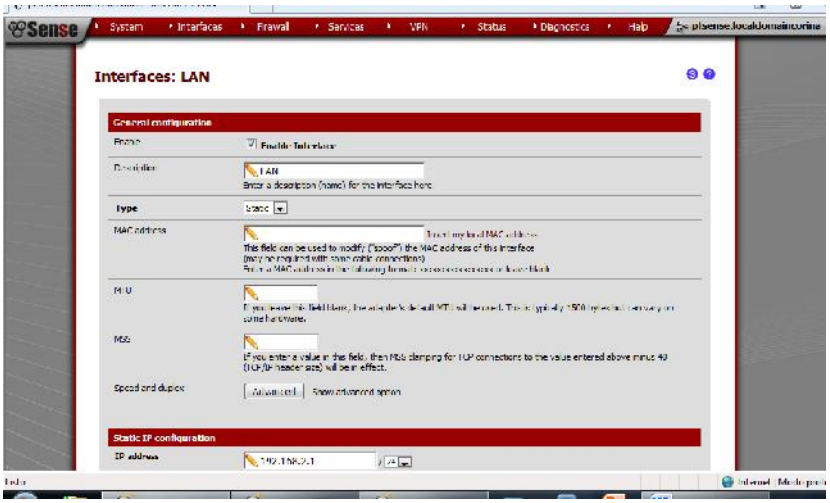


Figura IV.70. Configuración de interfaz Lan.

- Adicionalmente se puede cambiar la contraseña para ingresar al configurador Web del PfSense, si esta contraseña la olvidamos se puede cambiar con la opción 3 directamente desde el proxy.

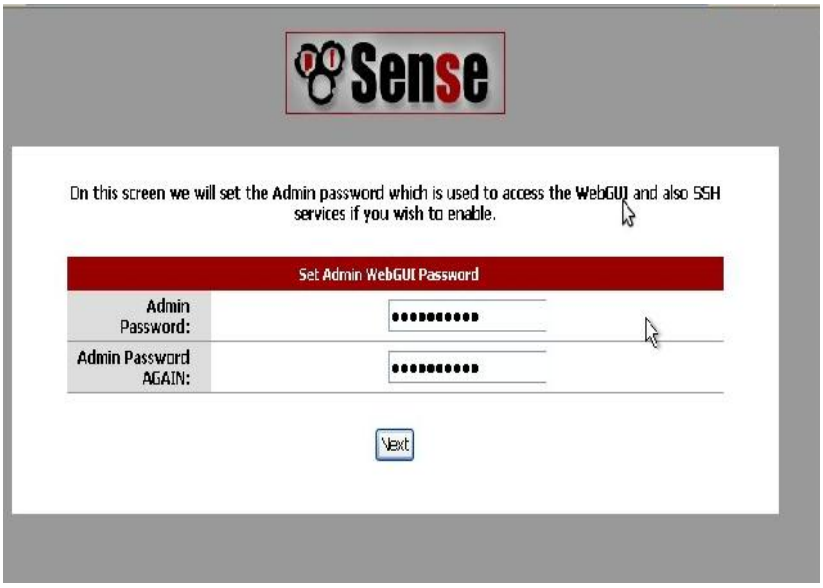


Figura IV.71. Cambio de contraseña para consola web.

- Pulsamos "reload", pedirá la nueva contraseña, y esperamos a que se realicen los cambios:

Figura IV.72. Registro de cambios con Reload.

4.3. CONFIGURACION DEL CORTAFUEGOS

- Ahora nos iremos a ***Firewall > NAT***, allí debemos seleccionar ***enable advanced outbound NAT***

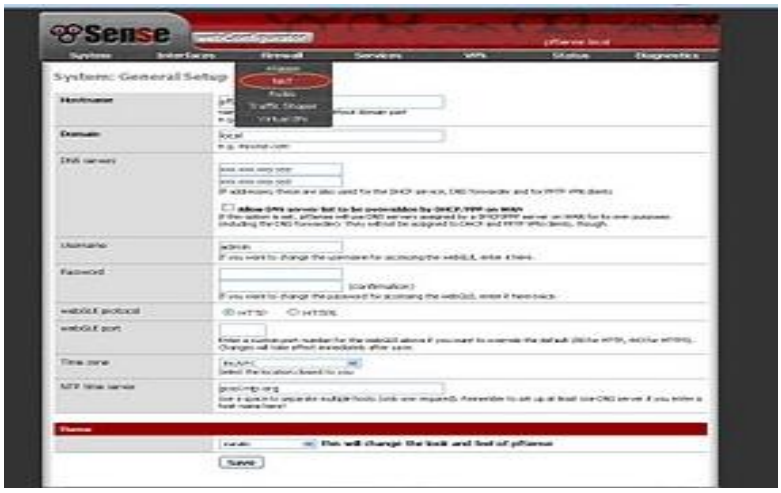


Figura IV.73. Configuración de Firewall

- Allí se borra todas las reglas que aparecen en la lista, esto es importante porque si no se hace el Firewall Transparente que queremos no funcionará. Se recomienda grabar los cambios en todo momento de la configuración.

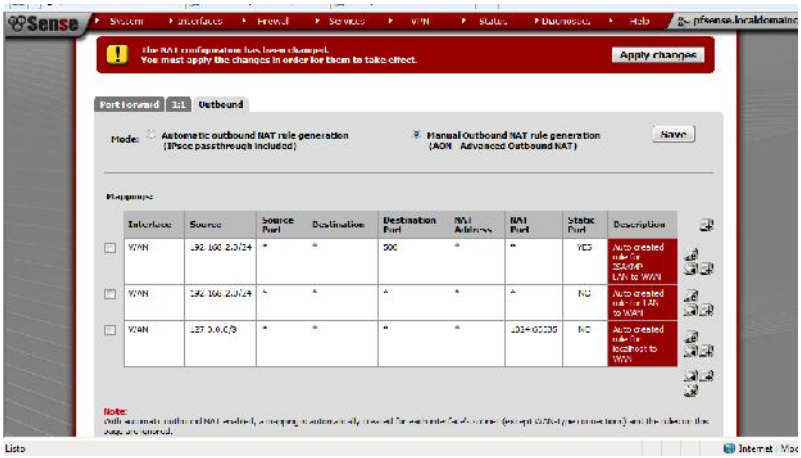


Figura IV.74. Reglas para dejar cortafuegos transparente.

- Cuando se tiene un servidor DHCP en la red LAN, desactivar el que trae pfsense, en ***Services > dhcp***, para que no entren en conflictos las máquinas con IPs duplicadas. Existen otros servicios como DNS, en ***Diagnostics*** esta opción para respaldar toda la configuración realizada si por algún motivo se tiene que generar de nuevo el pfsense ahorrando trabajo.

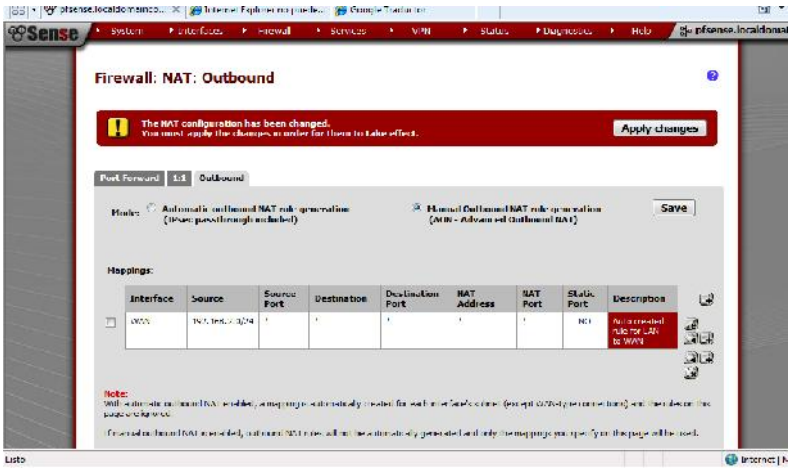


Figura IV.75. Verificación de reglas del firewall

- En ***Firewall > rules***, como se ve en la pestaña WAN no tiene ninguna regla, allí solo configurará reglas para DMZ y algunas conexiones entrantes

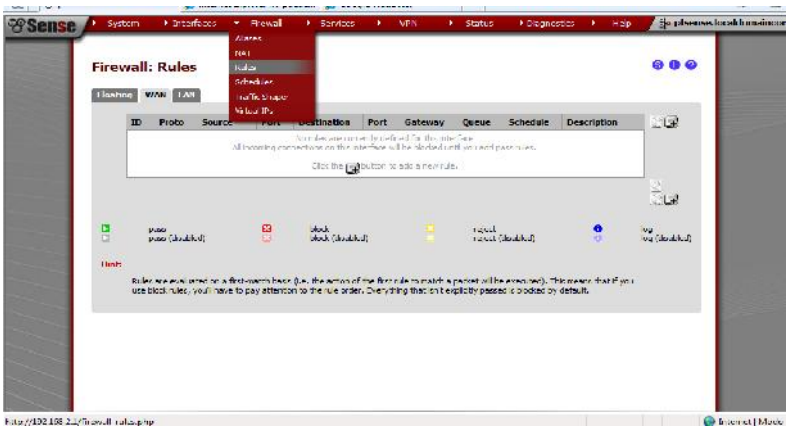


Figura IV.76. Selección de Firewall- Rules

- Haciendo clic sobre la pestaña LAN veremos que la regla por defecto es permitir todo el trafico de la red LAN, en este caso la editaremos y la desactivamos, pero primero añadiremos el tráfico que queremos dejar pasar (por defecto todo el trafico estará bloqueado), servicios tales como HTTP, HTTPS, SMTP, POP3, IMAP entre otros.

Figura IV.77. Desactiva regla por default de LAN

- Ya una vez añadido el conjunto de reglas que deseamos dejar pasar hacia internet, procedemos a editar la regla por defecto y la desactivamos, una vez aplicado los cambios esta se tornará atenuada con respecto a las otras.

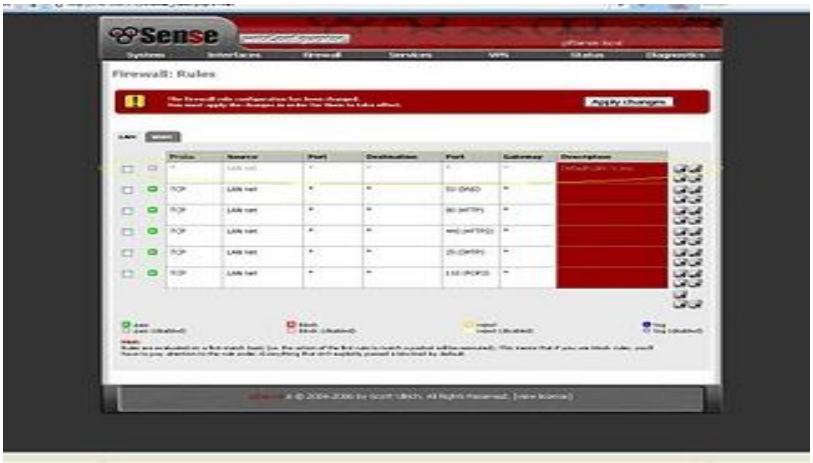


Figura IV.78. Regla por default atenuada.

4.4. CONFIGURACION DEL SERVIDOR PROXY

Luego de haber instalado el pfsense y configurado las interfaces, y cortafuegos nos dirigimos a instalar el paquete Squid, debido a que es uno de los servidores proxies más implementados a nivel mundial. Es un popular programa de software libre que implementa un servidor proxy y un dominio para caché de páginas web, publicado bajo licencia GPL; puede ser configurado para ser usado como proxy transparente de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. De modo predefinido Squid utiliza el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto disponible o bien que lo haga en varios puertos disponibles a la vez.

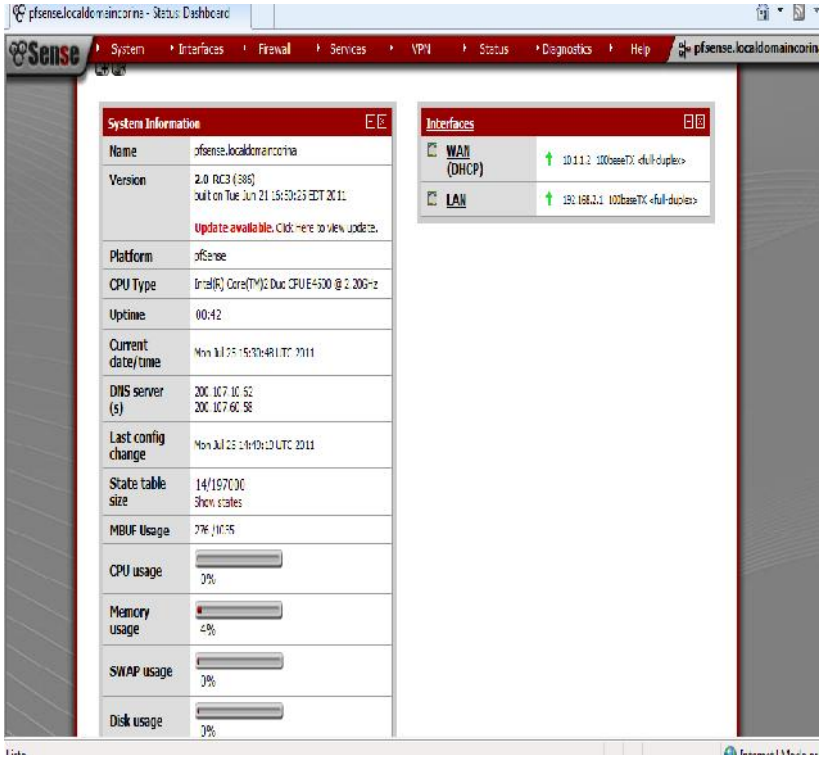


Figura IV.79. Información del sistema.

Para instalar el paquete, ingresamos al sitio web administrativo del pfsense, y

- Seleccionar en la pestaña ***System>Packages***, luego en ***Available Packages***, buscar en el listado de paquetes y agregar con el símbolo **"+"** ubicado a la derecha. Aceptar en la pregunta si queremos agregar el paquete a nuestra instalación.

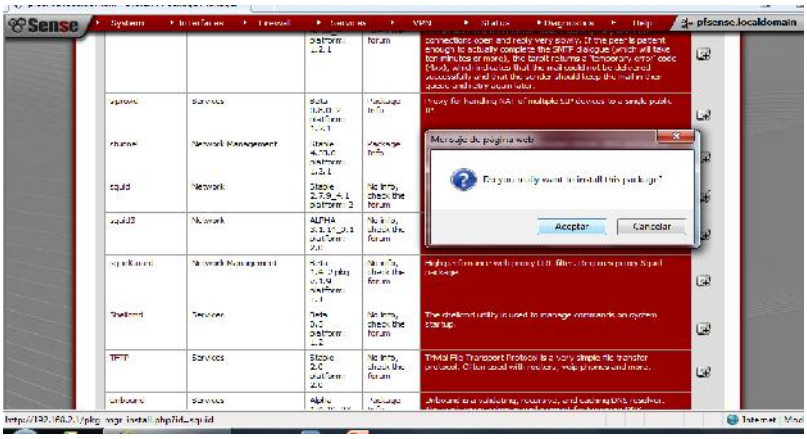


Figura IV.80. Selección del paquete Squid

- Esperar hasta que se complete el proceso de instalación.

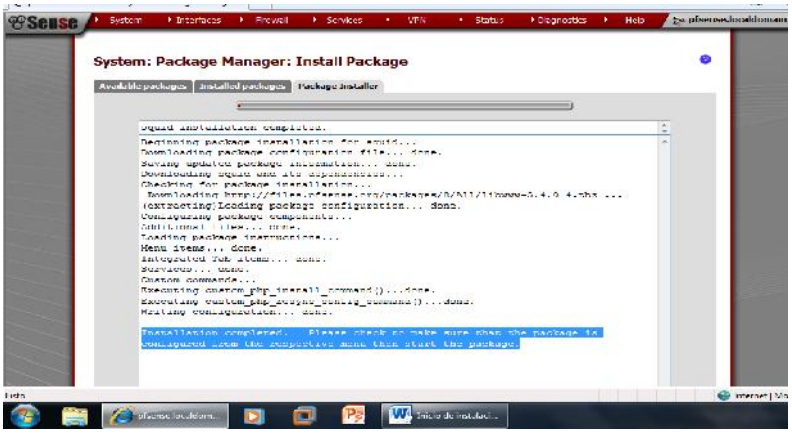


Figura IV.81. Avance del proceso de descarga de paquete.

- Luego de completar el proceso de instalación aparece el proxy instalado. Para entrar a configurar y crear restricciones en el servidor proxy, escoger ***Services>>Proxy Server.***

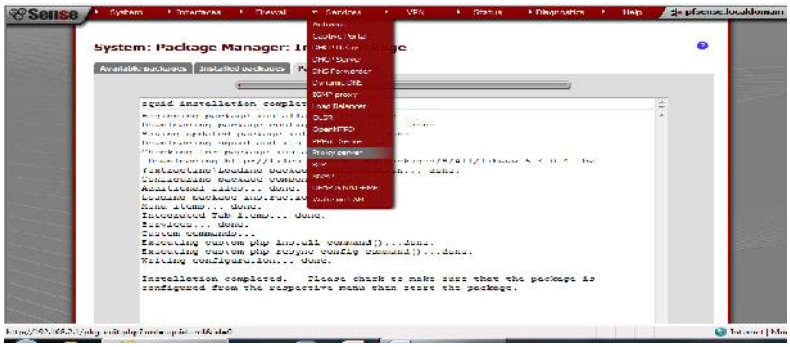


Figura IV.82. Servidor Proxy instalado.

- Ahora lo configuraremos squid según se necesite, así la interface, el tipo de proxy (en nuestro caso transparente), el puerto lo dejamos tal cual (3128), en modo transparente para que sea más fácil la integración de los equipos de la red local. También se indica cual será el nombre visible del host y nombre del administrador. El proxy siempre va a actuar en la interfaz de la red LAN. El resto de los parámetros se dejan por defecto y guardamos los cambios

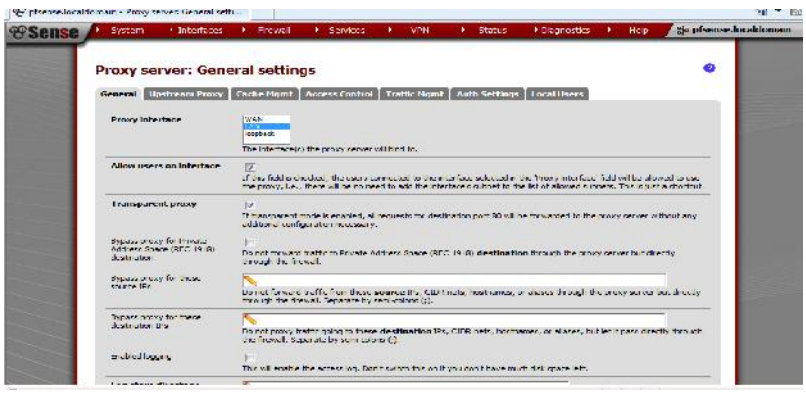


Figura IV.83. Configuración del Squid.

- Para la restricciones en el proxy seleccionar en la pestaña **Access Control** y en el parámetro **Blacklist** escribimos las páginas que queremos bloquear, una lista por ejemplo con los nombres facebook.com, youtube.com, playboy.com, etc., sin www, ni html.

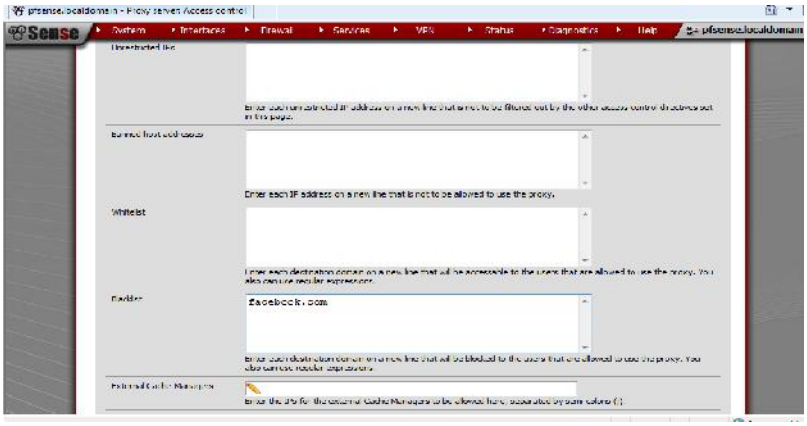


Figura IV.84. Configuración de restricciones en proxy.

- En la prueba de la restricción de la página verificamos si bloquea, para esto iniciar un navegador y escribir el nombre de una página a la que se desea acceder. Sale un error como se muestra en la siguiente imagen.

Figura IV.85. Verificación de restricción en página solicitada.

4.5. CONFIGURACION DEL PROXY FILTER

Squidguard es un filtro Web, funciona como "plugin" de Squid, es usado para restringir el acceso a Dominios/url's basado en una lista de control. Cuando SquidGuard recibe una solicitud, esta es examinada, y si esta dentro de la lista de prohibición es redirigida a la página de error. Principalmente SquidGuard basa su funcionamiento en listas de control y bases de datos de dominios, url's o expresiones.

- Seleccionar **en System >> Packages** y clic en SquidGuard del listado de paquetes. Esperar que se complete proceso de instalación y verificar que esté instalado.

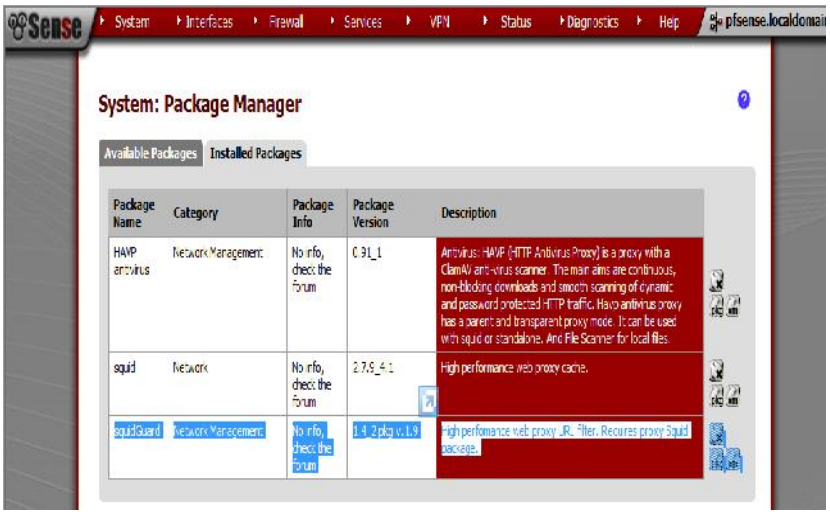


Figura IV.86. Selección de paquete SquidGuard para descarga

- En ***Services>> proxy filter***

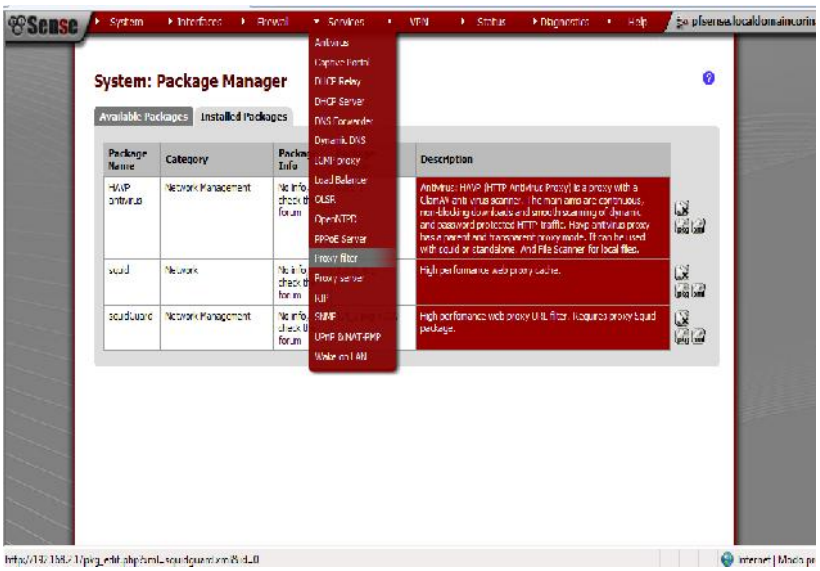


Figura IV.87. Opción services – proxy filter

- Habilitar el servicio y grabar los cambios.

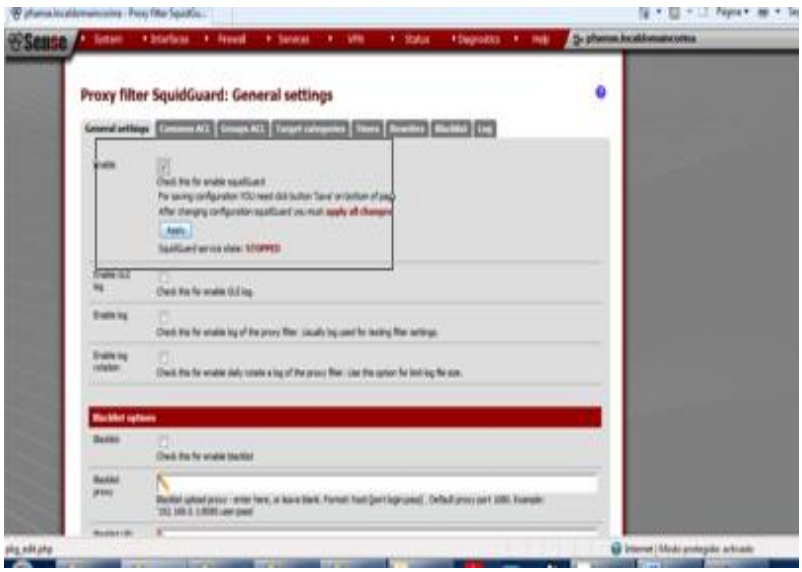


Figura IV.88. Grabar luego de habilitar servicio

- Al aplicar los cambios el servicio aparece habilitado.

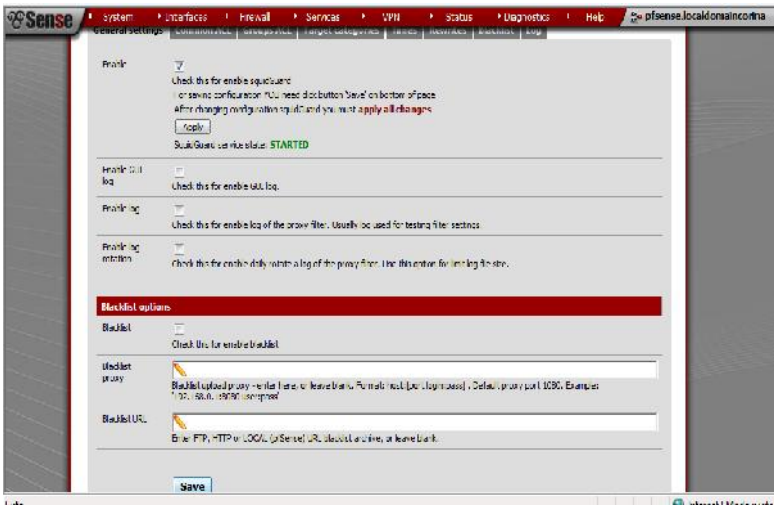


Figura IV.89. Servicio habilitado

- Por default toda la navegación en internet esta negada, no permite acceder a ninguna página como ilustra la imagen

Figura IV.90. Navegación negada por default.

- Para configurar el SquidGuard de acuerdo a necesidades en la ficha **Common ACL** en **Target Rules** dar clic a la flecha verde (para mostrar las reglas), buscamos la única que esta creada y cambiamos el tipo de acceso (por Allow) y grabar.

Figura IV.91. Habilita regla que esta creada

También grabar en **General Setup,** y podemos navegar normalmente

- Crear las reglas en ***Services>>Proxy Filter***, ficha ***Target Categories*** y agregamos una con el signo +, se puede indicar que no realice **la búsqueda de una palabra.**

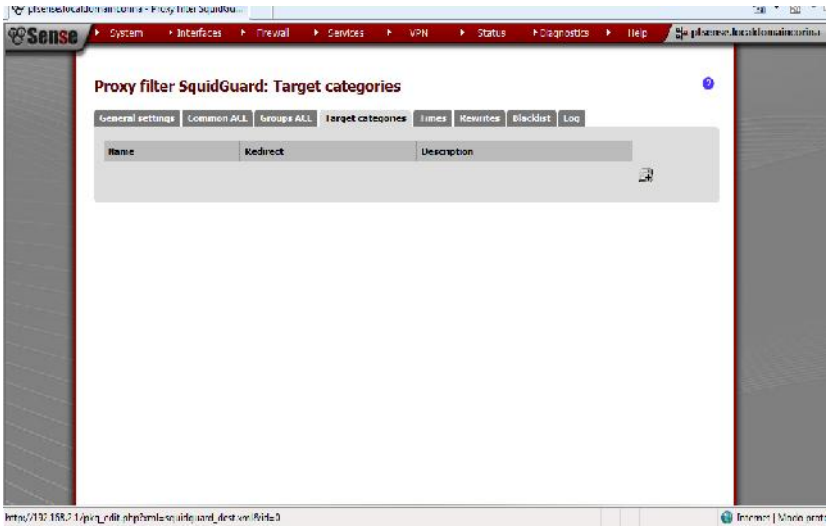


Figura IV.92. Creación de reglas

- Tenemos la pantalla

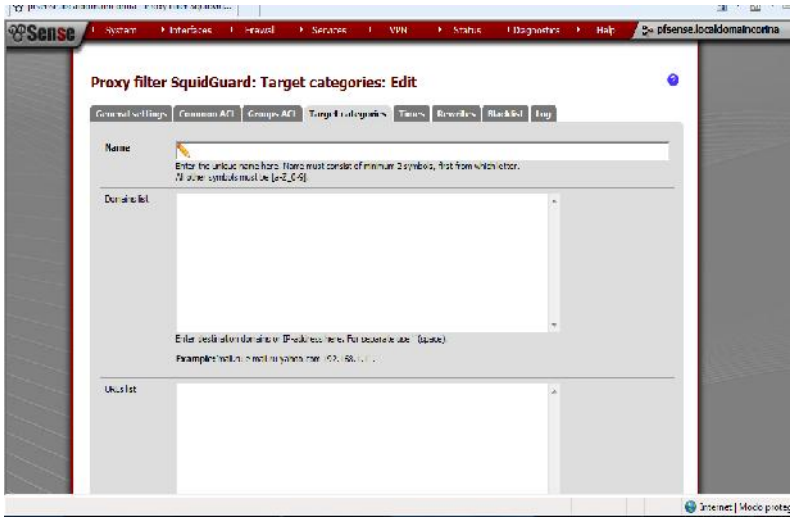


Figura IV.93. Edición de reglas.

- Especificar algunos valores:

  Name: Sitios_negados

  Domains list: nada

  URL's list: nada

  Expressions: '|xxx|sitiosporno|'

  Redirect mode: ext url move (enter URL)

  Redirect: www.google.com (La página a la que se redirige)

  Log: nada

  Descripción: Sitios denegados para los estudiantes del laboratorio#2

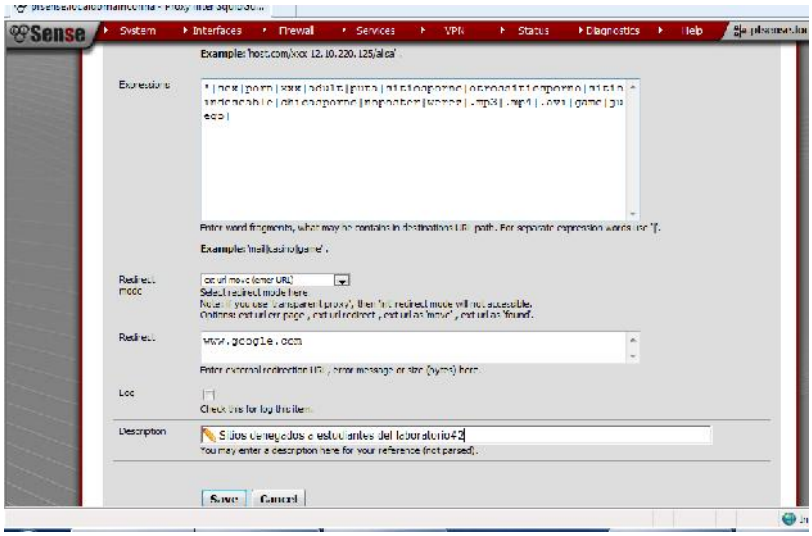


Figura IV.94. Expresiones de la regla de sitios_denegados.

- Grabar la regla quedaría así:

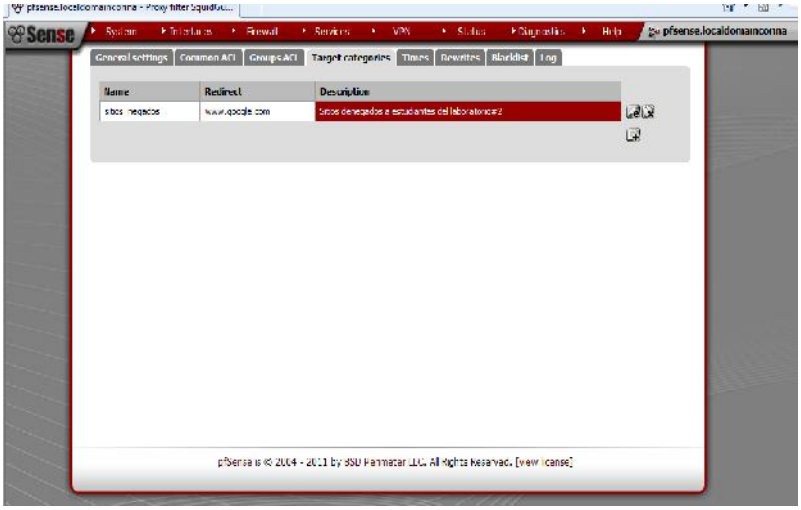


Figura IV.95. Regla de expresiones grabada.

- Para aplicar la regla en la ficha ***Common Acl***, localizamos en la lista y escoger el valor para denegar (deny). Configurar para permitir todas las búsquedas, excepto los sitios negados, y grabar también en ***"General settings"***

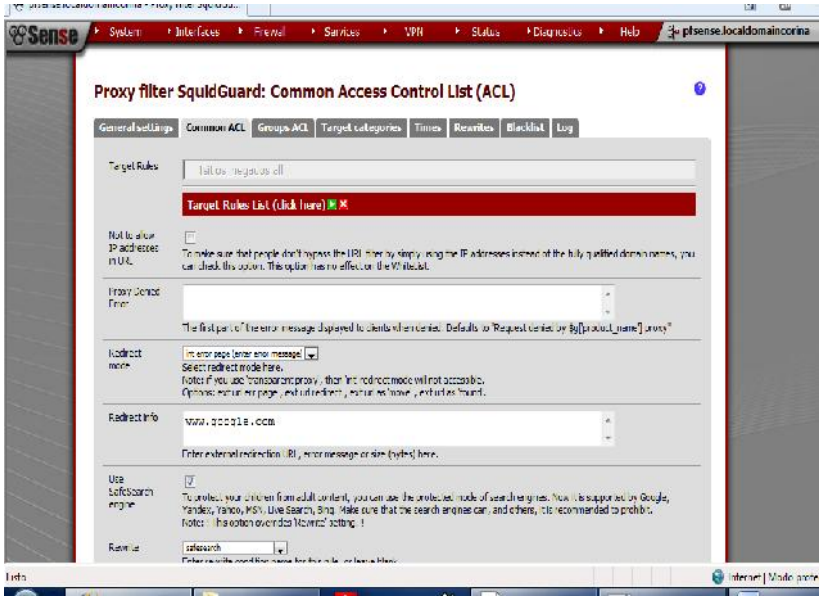


Figura IV.96. Aplicar regla de expresiones.

- Realizar la búsqueda de una de las frases bloqueadas.

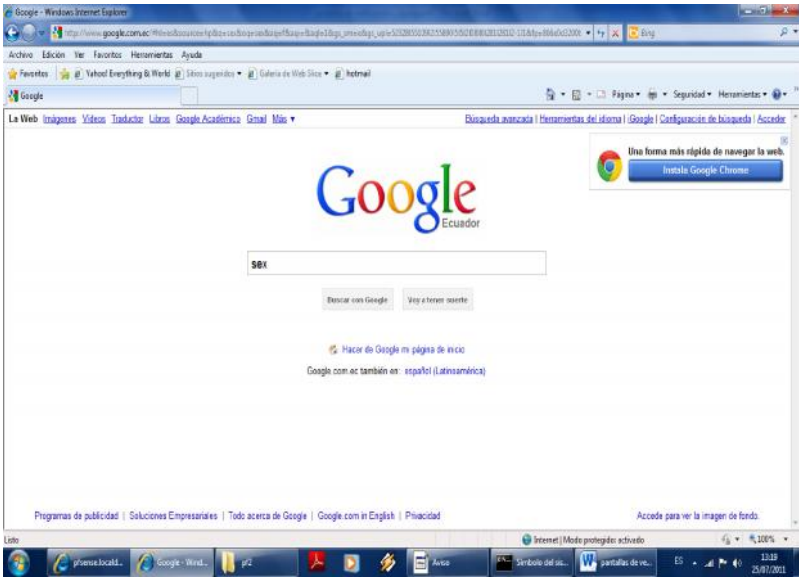


Figura IV.97. Búsqueda de frases negadas.

- No muestra nada y redirige al sitio http:// www.google.com. Igual si se busca juegos, mp3, computadoras, u otra.

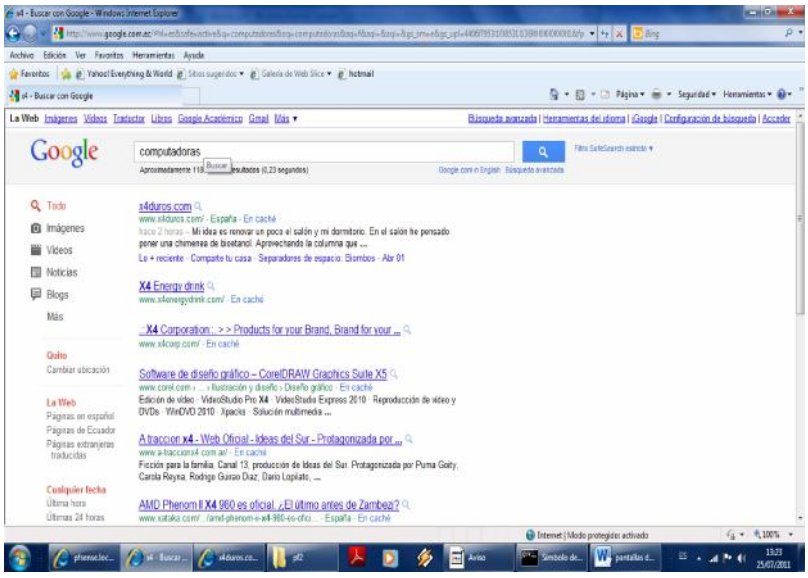


Figura IV.98. Verificación de búsqueda de frases restringidas.

- Se puede anotar más palabras o frases para configurarlo de acuerdo a o lo que requiera la institución, o agrupar dominios por categorías.

4.6 COMPROBACION DE LA HIPOTESIS.

El estudio de técnicas para el control de acceso a internet y su aplicación en la red de datos del Colegio "Corina Parral" si mejorará el control de acceso a la información que brinda el Internet.

CONCLUSIONES

- Con el estudio, análisis e implementación de una de las técnicas de control para el acceso a la información de internet si es posible controlar el acceso a sitios o páginas que ofrecen información ofensiva nada útil para estudiantes que realizan sus prácticas en los centros educativos, garantizando de esta manera que cuando ingresen a los computadores en horas de práctica de las diferentes asignaturas cuenten con el servicio de internet e ingresan a información agradable debido a la restricción para el acceso a páginas indebidas.

- El estudio e implementación de una técnica para el control de acceso a internet y su aplicación en la red de datos del Colegio "Corina Parral" si mejoró el control de acceso de los estudiantes de octavo de educación general básica a tercero de bachillerato a la información que brinda el Internet.

- Concientizar al personal encargado de laboratorios de prácticas de la importancia de controlar el acceso a la información que ofrece internet, ya que está demostrado que un porcentaje elevado de los fraudes informáticos proceden del interior de las propias organizaciones.

- Ningún cortafuego puede defenderse de manera automática contra cada amenaza nueva que surge. No se debe instalar un cortafuego una sola vez y esperar que lo proteja para siempre, hay que mantenerlo y actualizarlo.

RECOMENDACIONES

- En el equipo utilizado para el control de acceso a la información que ofrece internet es posible ubicar otra tarjeta de red, misma que permitiría aprovechar la otra línea que paga el plantel para internet, considerando que la línea de internet que brinda el gobierno a los centros educativos es inestable en el servicio.

- El proponer e implementar una de las técnicas de control para el acceso a internet requiere un alto compromiso con el centro educativo, constancia para renovar y actualizar la misma en relación el ambiente dinámico y el continuo avance de los programas y equipo que deben considerar los centros educativos; para el control y acceso a la información que ofrece internet en otras áreas o departamentos de la institución se requiere la aceptación de los usuarios porque se podría considerar como una violación a sus derechos, debe además normado en un manual de contingencia o en el reglamento interno de la institución.

- La seguridad informática e implementación de una técnica para acceder a internet no tiene una solución definitiva, se sugiere en los centros educativos que todo el personal encargado de los sistemas o laboratorios se innove de forma constante en tecnológica, para que este a la par del avance tecnológico que surge día a día.

- Finalmente en todas las empresas e instituciones educativas debe existir un documento (política de seguridad) conocido y firmado por todo el personal en el que consten diversos aspectos referentes a seguridad informática, como por ejemplo: se puede especificar desde cuantas letras o dígitos han de tener las contraseñas en los computadores de trabajo, las redes internas a las que pueden acceder, horario que tienen acceso a las redes sociales para evitar que se distraigan en su jornada de trabajo, que política existe para el acceso a recursos internos de la institución, entre otros. Además puede protegerse incorporando seguridad física, seguridad y educación para el usuario en su plan general.

RESUMEN

El estudio de técnicas de control para el acceso a la información que ofrece el internet, se realizó en un laboratorio de práctica del los estudiantes, está ubicado en el colegio "Corina Parral de Velasco Ibarra" de la ciudad de Chimbo, provincia de Bolívar.

En el desarrollo de la investigación se utilizaron los métodos deductivo e inductivo para descubrir las funcionalidades de los cortafuegos, servidores proxy, y lo referente a licencia, funcionalidades, instalación, componentes básicos, y configuración básica de las herramientas Squid y Pfsense. Se implementó Pfsense versión 2.0, una distribución de software libre sobre un computador Intel Core 2 Duo con 2GB de memoria ram, puede ser administrado remotamente y está dedicado única y exclusivamente para el control de acceso a la información en el laboratorio del plantel.

Como resultado de la investigación se controlo el acceso a sitios de internet que ofrecen información ofensiva en un 80% así también se logró restringir el acceso a páginas que distraen e impiden la atención total de los estudiantes en las diferentes horas de práctica, como son las redes sociales.

En definitiva fue posible implementar una técnica de control de acceso a la información que ofrece a internet, se desarrollo bajo software libre, a un mínimo costo, de forma trasparente para los usuarios y de mantenimiento sencillo. Se recomienda previa autorización o política de la institución su aplicación en otros laboratorios de práctica de los estudiantes, así como en diferentes áreas académicas o departamentos del plantel.

SUMARRY

The study of control techniques for access to information provided by the internet was conducted in a laboratory for student practice, which is located in the "Corina Parral de Velasco Ibarra" school, city of Chimbo, Bolivar Province.

In the development of research methods were used deductive and inductive to discover the capabilities of firewalls, proxies, and the license terms, features, installation, basic components and basic configuration of Squid and Pfsense tools. Implemented Pfsense 2.0, a distribution of free software on a PC Intel Core 2 Duo with 2 GB of RAM, can be administered remotely and is dedicated exclusively to control access to information in the laboratory on campus.

As a result of the investigation was controlled access to internet sites that offer information offensive in 80%, so it was possible to restrict access to pages that are distracting and impede the full attention of students at different hours of practice, such as social networks.

Ultimately it was possible to implement a technique for controlling access to the information offered to the internet, software development under free, at minimal cost, transparently to users and easy to maintain. We recommend prior authorization or institutional policy implementation in others laboratories in student practice and in academic areas and departments on campus.

GLOSARIO

ARP: utiliza un cache que consiste en una tabla que almacena las asignaciones entre nivel de enlace de datos y las direcciones IP del nivel de red. El nivel de enlace de datos se encarga de gestionar las direcciones MAC y el nivel de red de las direcciones IP. ARP asocia direcciones IP a las direcciones MAC.

DHCP: es un protocolo que permite a dispositivos individuales en una red de direcciones IP obtener su propia información de configuración de red (dirección IP; mascara de sub-red, puerta de enlace, etc.) a partir de un servidor DHCP. Su propósito principal es hacer más fácil administrar las redes grandes. DHCP existe desde 1993 como protocolo estándar y se describe a detalle en el RFC 2131. Sin la ayuda de un servidor DHCP, tendrían que configurarse de forma manual cada dirección IP de cada anfitrión que pertenezca a una red de Área Local.

DNS: es una base de datos distribuida y jerárquica que almacena la información necesaria para los nombres de dominio. Sus usos principales son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico correspondientes para cada dominio. El DNS nació de la necesidad de facilitar a los seres humanos el acceso hacia los servidores disponibles a través de Internet permitiendo hacerlo por un nombre, más fácil de recordar que una dirección IP.

FIREWALL: Dispositivo que se coloca antes del router o modem y que filtra los contenidos que entran y salen del exterior, con el fin de proteger los recursos de una red privada de usuarios de redes externas.

FTP: es uno de los protocolos estándar más utilizados en Internet siendo idóneo para la transferencia de grandes bloques de datos a través de redes que soporten TCP/IP. El servicio utiliza los puertos 20 y 21, exclusivamente sobre TCP. El puerto 20 es utilizado para el flujo de datos entre cliente y servidor. El puerto 21 es utilizando para el envío de órdenes del cliente hacia el servidor. Prácticamente todos los sistemas operativos y plataformas incluyen soporte para FTP, lo que permite que cualquier computadora conectada a una red basada sobre TCP/IP pueda hacer uso de este servicio a través de un cliente FTP.

GNU: Proyecto para desarrollar un sistema operativo del mismo nombre, compuesto íntegramente por software libre, y publicado bajo licencia GPL.

GPL: Licencia utilizada para la publicación de programas del proyecto GNU, que permite libre copia, modificación y distribución mientras se incluya el código fuente y se ofrezcan dichos derechos también sobre éste. Además la licencia debe aplicarse a cualquier producto basado en su código, conservando de esta forma los derechos de los usuarios de forma continua.

IP: realiza la tarea básica de capturar los paquetes de datos desde una fuente hacia un destino. El propósito principal de IP es proveer una dirección única a cada sistema para asegurar que una computadora en Internet pueda identificar a otra.

IPv4: es la versión 4 del Protocolo de Internet, es el principal protocolo utilizado en el Nivel de Red del Modelo TCP/IP para Internet. Sin embargo, muchas de estas están reservadas para propósitos especiales como redes privadas, Multidifusión (Multicast), etc.

IPv6: Protocolo de Internet versión 6, surgió por la necesidad de ampliar el número de direcciones IPs, como reemplazo del protocolo IPv4. IPv6 tiene como objetivo solucionar el problema concerniente al límite de direcciones IP que se pueden asignar a través de IPv4, las cuales tendrán mucha demanda en un futuro no muy lejano cuando se incrementen el número de teléfonos móviles y otros dispositivos de comunicación que ofrezcan acceso hacia Internet

IPTABLES: es el nombre de la herramienta de espacio de usuario (User Space, es decir, área de memoria donde todas las aplicaciones, en modo de usuario, pueden ser intercambiadas hacia memoria virtual cuando sea necesario) a través de la cual los administradores crean reglas para cada filtrado de paquetes y módulos de NAT. Iptables es la herramienta estándar de todas las distribuciones modernas de GNU/Linux.

FreeBSD: es un sistema operativo libre para computadoras basado en las CPU de arquitectura Intel, incluyendo procesadores 386, 486 (versiones SX y DX), y Pentium. También funciona en procesadores compatibles con Intel como AMD y Cyrix. Actualmente también es posible utilizarlo hasta en once arquitecturas distintas como Alpha, AMD64, IA-64, MIPS, PowerPC y UltraSPARC.

LINUX: Un sistema Operativo, es una implementación de libre distribución UNIX para computadoras personales , servidores, y estaciones de trabajo. Fue desarrollado para el i386 y ahora soporta los procesadores i486, Pentium, Pentium Pro y Pentium II, así como los clones AMD y Cyrix. También soporta máquinas basadas en SPARC, DEC Alpha, PowerPC/PowerMac, y Mac/Amiga Motorola 680x0. Es muy eficiente y tiene un excelente diseño. Es multitarea, multiusuario, multiplataforma y multiprocesador; en las plataformas Intel corre en modo protegido.

En sus orígenes fue desarrollado, en 1990, por el informático finlandés Linus Torvalds, que publicó su código como un denominado código abierto, esto es, accesible para toda la comunidad, sin restricciones para modificarlo y ampliarlo. Este planteamiento, favorecido por su estructura modular (basado en la instalación de diversos paquetes), generó una nueva visión de desarrollo informático, ya que su expansión fue debida a la aportación, generalmente voluntaria y sin ánimo de lucro, de multitud de desarrolladores independientes.

NAT: La traducción de direcciones de red (NAT, Network Address Translation) también es conocida como enmascaramiento de IPs. Es una técnica mediante la cual las

direcciones fuente o destino de los paquetes IP son reescritas, sustituidas por otras (de ahí el "enmascaramiento").

NIC: es una institución encargada de asignar los nombres de dominio en Internet, ya sean nombres de dominio genéricos o por países, permitiendo a personas o empresas montar sitios de Internet a través de un ISP mediante un DNS. Técnicamente existe un NIC por cada país en el mundo y cada uno de estos es responsable por todos los dominios con la terminación correspondiente a su país. Por ejemplo: NIC Ecuador es la entidad encargada de gestionar todos los dominios con terminación .ec, la cual es la terminación correspondiente asignada a los dominios de Ecuador.

MÁSCARA DE RED: Número de bits que indica el rango de direcciones IP que residen en una sola red, subred o superred.

PROXY: se define como una computadora o dispositivo que ofrece un servicio de red que consiste en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red, es decir un proxy realiza una acción en representación de otro. Un proxy permite tener control sobre la navegación en internet. Su finalidad más habitual es la que sirve para interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc.

PUERTO: Un canal de comunicación para computadores en una red.

RFC: Son conjuntos de notas técnicas y de organización que se elaboran desde 1969 donde se describen los estándares o recomendaciones de Internet, antes ARPANET. Ejemplos de esto son los usos del Retorno del sistema (loopback, RFC 1643), las redes privadas (RFC 1918).

ROUTER: es un dispositivo que envía paquetes de datos a través de redes informáticas. Un router está conectado a dos o más líneas de datos de distintas redes.
Cuando los datos se presentan en una de las líneas, el router lee la información de dirección en el paquete para determinar su destino final. Luego, utilizando la información en su tabla de enrutamiento, que dirige el paquete a la red siguiente de su viaje o descarta el paquete. Un paquete de datos por lo general pasan de un router a través de las redes de Internet hasta que llegue a su equipo de destino a menos que la dirección IP de origen está en una red privada.

SOFTWARE LIBRE: se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. Cuando se habla de software libre, es mejor evitar términos como: `regalar' o `gratis', porque esos términos implican que lo importante es el precio, y no la libertad.

SSH: es un conjunto de estándares y protocolo de red que permite establecer una comunicación a través de un canal seguro entre un cliente local y un servidor remoto. Utiliza una clave pública cifrada para autenticar el servidor remoto y, opcionalmente, permitir al servidor remoto autenticar al usuario. SSH provee confidencialidad e integridad en la transferencia de los datos utilizando criptografía y MAC (Message

Authentication Codes, o Códigos de Autenticación de Mensaje). De modo predeterminado, escucha peticiones a través del puerto 22 por TCP.

TCP/IP: es la plataforma que sostiene Internet y que permite la comunicación entre sistemas operativos en diferentes computadoras, ya sea sobre redes de área local (LAN) o redes de área extensa (WAN). Es un protocolo orientado hacia conexión que resuelve numerosos problemas de fiabilidad para proveer una transmisión de bytes fiable, ya que se encarga de que los datos lleguen en orden, tenga un mínimo de correcciones de errores, se descarten datos duplicados, se vuelvan a enviar los paquetes perdidos o descartados e incluya control de congestión de tráfico.

UDP: es un protocolo de datagrama sin corrección; no provee las garantías de fiabilidad y ordenamiento de TCP a los protocolos del Nivel de Aplicación y los datagramas pueden llegar en desorden o perderse sin notificación. Como consecuencia de lo anterior es que UDP es un protocolo más rápido y eficiente para tareas ligeras o sensibles al tiempo una interfaz muy simple entre el Nivel de Red y Nivel de Aplicación. Si se requiere algún tipo de fiabilidad para los datos transmitidos, esta debe ser implementada en los niveles superiores de la pila.

UNIX: Es un sistema operativo de tiempo compartido, controla los recursos de una computadora y los asigna entre los usuarios. Permite a los usuarios correr sus programas. Controla los dispositivos de periféricos conectados a la máquina.

Este sistema fue desarrollado originalmente por Ken Thompson y Dennis Ritchie en los Bell Laboratories en 1969 para su uso en minicomputadoras. Tiene diversas variantes y

se considera potente, más transportable e independiente de equipos concretos que otros sistemas operativos porque está escrito en lenguaje C.

Desde el principio se concibió como un sistema abierto, cediéndose su uso libremente a instituciones gubernamentales y académicas, ámbitos en los que llegó a ser muy popular. Todo esto contribuyó a que se desarrollase una gran cantidad de aplicaciones comerciales en este entorno y a que muchas empresas se dedicasen a su explotación comercial tras su liberalización, en 1984. El UNIX está disponible en varias formas, entre las que se encuentran AIX, una versión de UNIX adaptada por IBM (para su uso en estaciones de trabajo basadas en RISC), Solaris, versión de Sun, A/UX (versión gráfica para equipos Apple Macintosh) y Linux, la versión de UNIX más reciente y popular que se ejecuta en una gran variedad de plataformas que van desde los PC x86 a PowerPC, pasando por la diversidad de máquinas de IBM

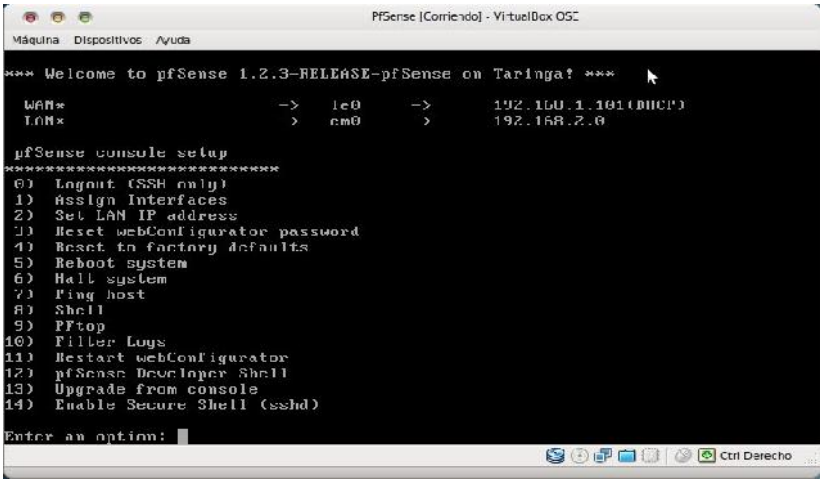
ANEXOS

ANEXOS A

MANUAL DE CONSOLA DE PFSENSE

Para administrar el firewall instalado en el laboratorio # 2 del Plantel se presenta un resumen de las opciones de la consola que tenemos en el servidor, así:

La consola puede ser manejada mediante el teclado o usando un cliente SSH, a continuación se muestra una imagen de la consola en tiempo real, puede variar dependiendo de la versión.



0) <u>Logout (SSH only)</u>

Sale de la conexión al puerto 22 SSH (SSH, son las siglas de Secure Shell) de nuestro proxy, recordemos que primero tenemos que habilitar este servicio, el cual se autoriza desde el WebGUI (System-->>Advance-->>Secure Shell).

Cuando está habilitado este servicio, solamente se accede a la consola tal cual si estuviese frente a la máquina físicamente, la ventaja de esto es que podemos retirar el teclado del proxy y administrarlo remotamente, pero con las opciones de “consola”, para cuando no se pueda acceder al WebGUI o realizar tareas básicas.

1) Assign Interfaces

Esta opción sirve para reiniciar las interfaces que tenemos asignadas o reconfigurarlas, tal como se hizo al instalar el sistema, identificándolas por medio de su MAC address. Pueden utilizar esta página para conocer la MAC Address de http://www.8086.net/tools/mac/

2) Set LAN IP Address

Se utiliza para cambiar el rango de IPs, reconfigurarlas, activar el servicio DHCP en la interface LAN, cambiar el rango del DHCP, y también para cambiar la máscara de subred. Esto sirve también cuando está bloqueado el WebGUI.

3) Reset webConfigurator password

Esta opción restaura la contraseña del WebGUI, por la de default:

1. Usuario: admin
2. Contraseña: pfsense

4) Reset to factory defaults

Restaura la configuración del sistema por la de fábrica. Todos los paquetes instalados, configuraciones de reglas, interfaces asignadas, logs, que pueden provocar inestabilidad en el sistema son borrados.

Se puede hacer esto también desde (Diagnostics-->>Factory Defaults)

5) Reboot system

Reinicia el sistema, una vez que se confirma realizar la operación.

6) Halt system

Apaga el sistema, igualmente mediante confirmación del administrador.

7) Ping host

Solicita la dirección IP o el nombre del host, para realizar un ping (para comprobar el estado de la conexión.

8) Shell

Accede al intérprete de comandos Unix, para ejecutar herramientas de diagnóstico.

9) Pftop

Utilidad para visualizar en tiempo real los estados activos y estadísticas para pf (filtro de paquetes) de OpenBSD.

10) Filter logs

Muestra la información en tiempo real del filtro, también se puede acceder a esta por medio del WebGUI (Status-->>System logs) es mejor acceder a ella por medio del WebGUI.

11) Restart webConfigurator

Es utilizado en las ocasiones que el WebGUI es inaccesible o se han generado errores y se quiere volver a reiniciar la configuración.

12) PfSense Developer Shell

Interprete de código PHP, es usado por los desarrolladores para probar nuevos módulos, su principal objetivo es que los desarrolladores se adapten a código base de PfSense.

13) Upgrade from console

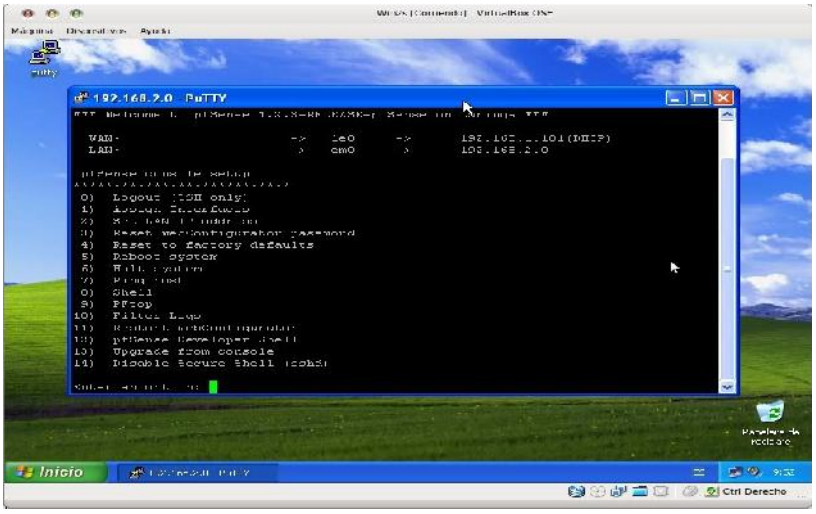
Con esta opción se actualiza el firmware o versión del sistema, puede ser mediante una URL u otra ruta.

También se puede realizar esto mediante el WebGUI (System-->>Firmware)

14) Disable secure shell (sshd)

Habilita o deshabilita el demonio sshd, obligando la administración solamente desde el WebGUI, y haciendo menos vulnerable nuestro firewall.

Para realizar la conexión SSH, desde Windows se recomienda PUTTY, que también sirve para Linux, pero para eso mejor la consola (ssh usuario_remoto@host_remoto) desde la red LAN.



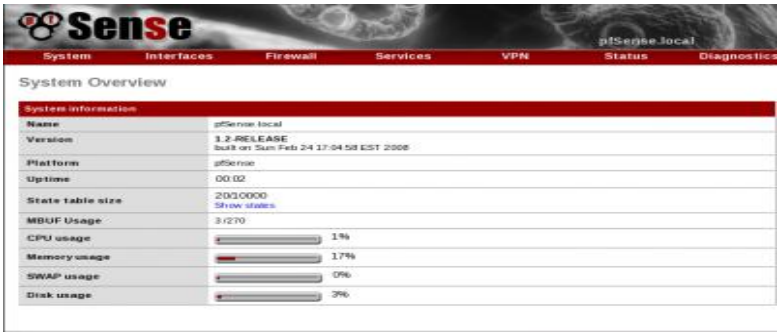
ANEXOS B

MANUAL DE ADMINISTRACION DESDE LA WEB PFSENSE

A continuación se presente las diferentes opciones que contiene pfSense:

Inicio

Esta será la primera pantalla que nos encontraremos al entrar en la web de Pfsense, Desde ella podremos observar en tiempo real alguna estadísticas de interés.



SYSTEM

- ***Advanced***. Se utiliza para configurar temas de seguridad como pueden ser la comunicación ssh, uso de certificados, tuneling, etc.

- ***Firmware***. Es utilizado para la realización de actualizaciones.

- ***General setup***. Permite realizar cambios en la configuración realizada al principio (Configuración Básica).

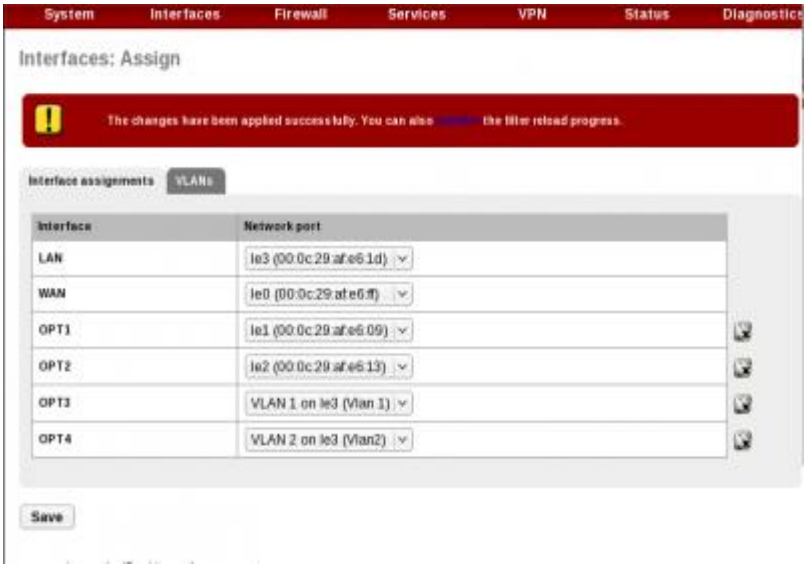
- ***Package***. Esta opción es utilizada para poder observar e instalar paquetes en Pfsense.

- ***Setup wizard***. lleva a la configuración guiada.

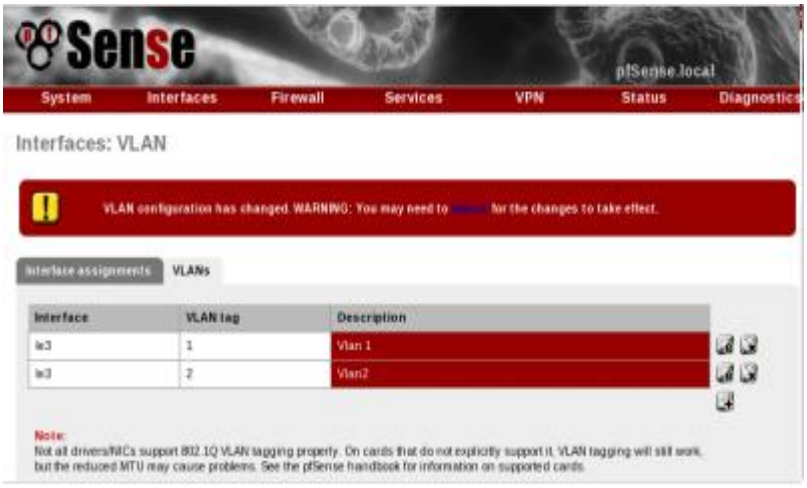
- ***Static router***. Aquí tendremos la posibilidad de configurar de manera estática las tablas de ruteo.

INTERFACES

- ***Assigns***. Sirve para la asignación de nuevas interfaces.

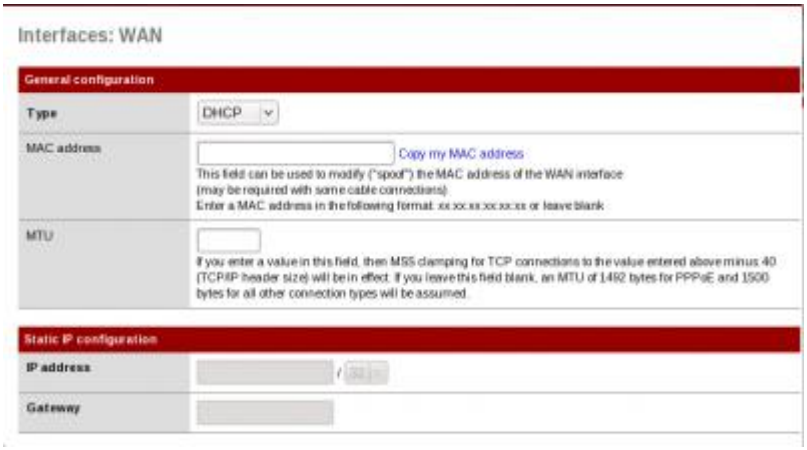


Aquí también podremos añadir nuevas Vlans:

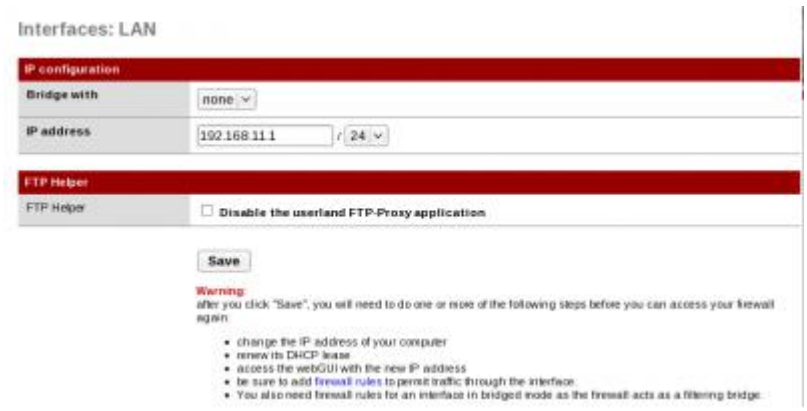


Para hacer una Vlan pulsamos en el "+" y rellenamos la siguiente pantalla:

- ***WAN***. Aquí podremos configurar la interface WAN.



- ***LAN***. Aquí podremos configurar la interface LAN.



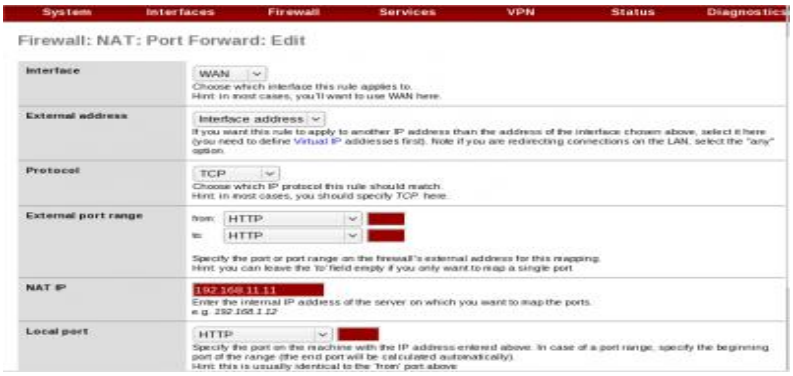
- ***OPT***. Aquí podremos configurar las distintas interfaces OPT.

FIREWALL

- ***Aliases***. Aquí tenemos la oportunidad de agrupar puertos e IPs bajo el uso de alias.

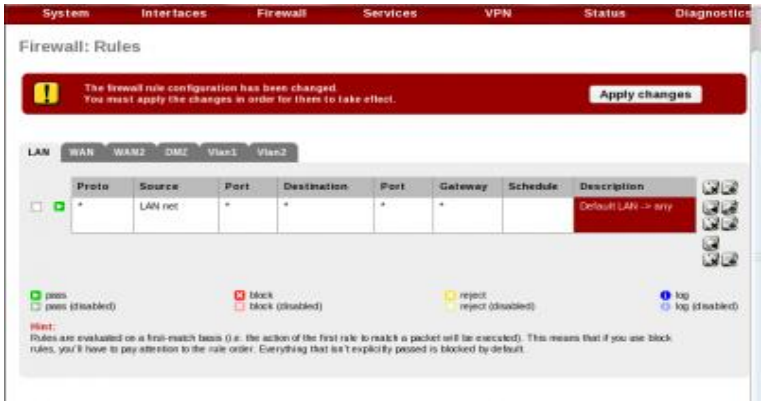
- ***NAT port Forward***. Da la oportunidad de realizar el redireccionamiento NAT.

Las reglas NAT se añaden pulsando '+' y rellenando el siguiente formulario:



- ***NAT Outbound***. Gracias a esto podremos configurar todo lo referente a las salidas del NAT.

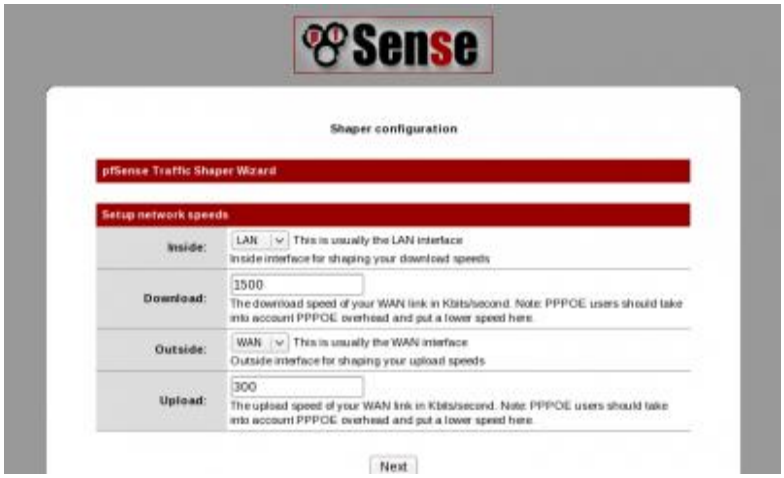
- ***Rules***. Aquí definiremos las reglas que deseamos para nuestro Firewall, estas reglas se definirán de forma separada para cada una de las interfaces.



- ***Schedules***. Aquí podremos ver las listas de reglas de firewall.

- ***Traffic Shaper***. Sirve para la configuración del regulador de caudal, esta tarea se realizará rellenando una serie de cuestionarios que pfsense nos ofrecerá de forma guiada.

Aquí tendremos que indicar cuál será la interface interna y externa que queremos regular y cuáles serán sus anchos de banda de subida y bajada.

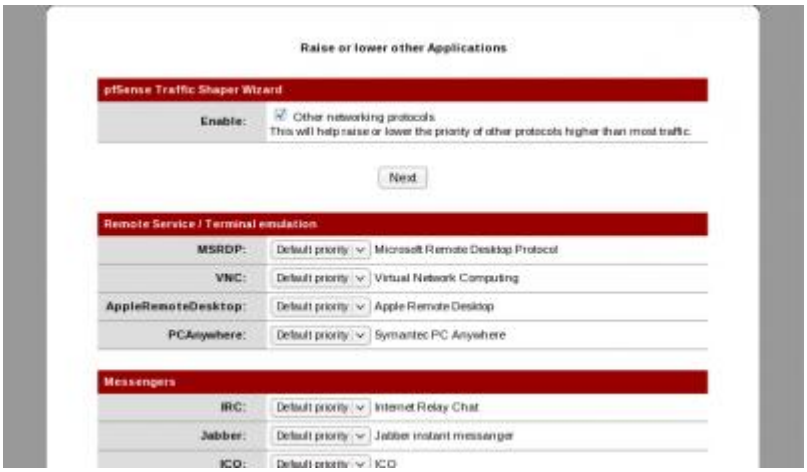


Luego se nos pregunta si queremos dar preferencia a comunicaciones VoIP:

Después podremos configurar todo lo referente a descargas P2P:

También podremos decidir si queremos dar o no preferencias a juegos vía Internet:

Por último se nos dará la oportunidad de configurar el resto de prioridades de tráfico.



Y al final de todo nos saldrá una pantalla de confirmación:

- ***Virtual Ip addresses***. Aquí podremos configurar todo lo referente a direcciones IP virtuales.

SERVICES

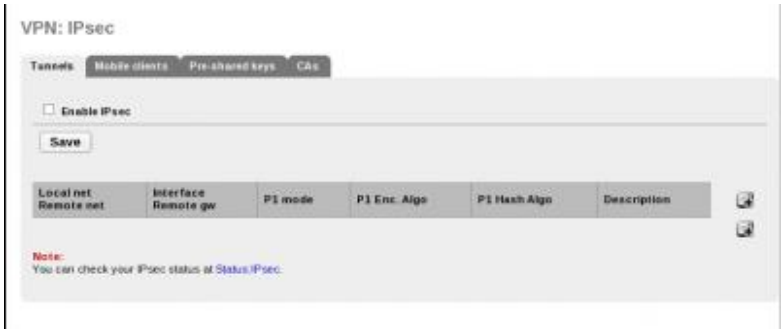
- ***Captive portal***. Permite configurar como los usuarios de una red pueden navegar por Internet.
- ***DNS forwarder***. Para configurar todo lo referente al servidor DNS, como los servidores DNS por defecto, o el uso del nuestro propio para asignar a las direcciones ips nuestras direcciones DNS.
- ***DHCP relay***. Servicio que permite que todas las peticiones DCHP que lleguen a un sean reenviadas hacia el otro equipo.
- ***DHCP Server***. Aquí se puede configurar todo lo concerniente al servicio DCHP ofertado por Pfsense.
- ***Dynamic DNS***. Permite la actualización en tiempo real de la información sobre nombres de dominio.
- ***Load Balancer***. Aquí podremos configurar todo lo referente al balanceo de carga, para ello debemos crear un pool como viene en la siguiente pantalla:

- ***OLSR***. Esto es utilizado para el establecimiento de conexiones entre nodos de una red inalámbrica.
- ***PPPoE Server***. Servidor para el encapsulamiento de paquetes PPP a Ethernet.

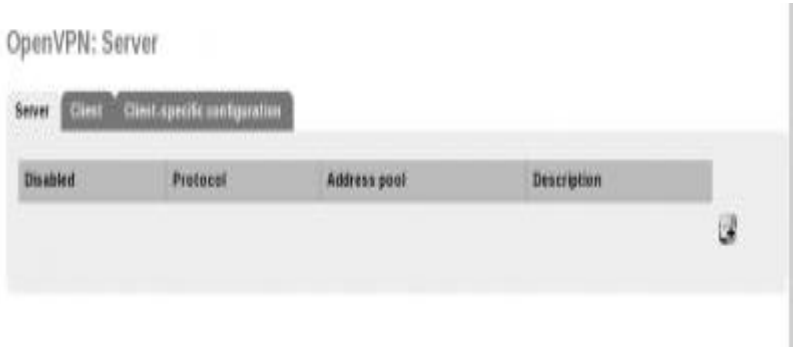
- ***RIP***. Aquí podremos habilitar el protocolo RIP para el todo lo referente al ruteo.
- ***SNMP***. Aquí podremos montar un servicio de correo mediante el uso del protocolo SNMP.
- ***UPnP***. Utilizado para intercambio de información entre los dispositivos de la red.
- ***OpenNTPD***. Permite la sincronización de los sistemas.
- ***Wake on LAN***. Permite encender de forma remota máquinas apagadas.

VPN

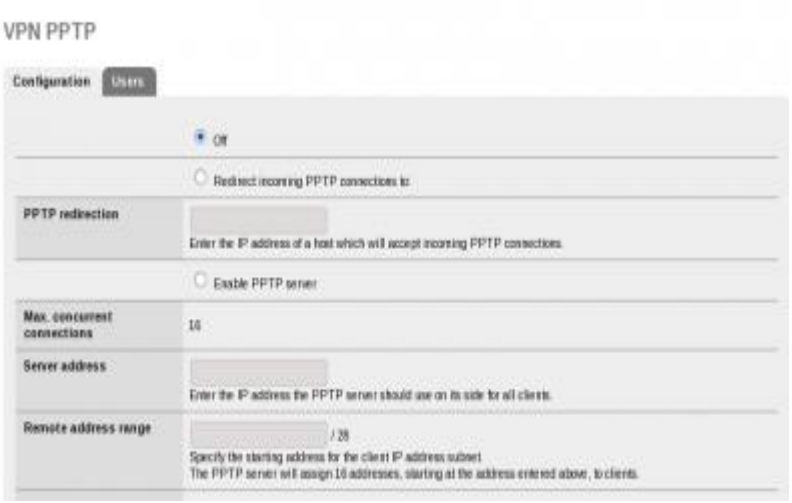
- ***IPsec***. Aquí podremos definir las reglas Ipsec:



- ***OpenVPNserver***. Para crear redes privadas virtuales.



- ***PPTP***. Aquí podremos realizar la implementación de la red privada virtual propiamente dicha.



STATUS

En status podremos ver estadísticas y datos de todo el sistema sus pestañas son:

- ***CARP***. Protocolo que permite que múltiples equipos en la misma red local compartan una o más direcciones IP.
- ***DHCP leases***. Datos sobre el servicio DCHP
- ***Filter Reload***. Reglas de filtrado
- ***Interfaces***. Datos sobre las interfaces
- ***Ipsec***. Datos sobre la configuración Ipsec
- ***Load Balancer***. Datos sobre el balanceo de carga
- ***Package logs***. Datos sobre los paquetes
- ***Queues***. Datos sobre las colas

- ***RRD Graphs***. Gráficos de los RRD
- ***Services***. Datos a cerca de los servicios
- ***System***. Datos del sistema
- ***System logs***. Datos de los logs generados
- ***Traffic graph***. Datos del tráfico de red
- ***UPnP***. Datos a cerca de UPnP

DIAGNOSTICS

Las posibles opciones que podemos utilizar son:

- ***ARP Tables.*** Aquí podremos ver la tabla ARP.
- ***Command.*** Desde aquí podremos ejecutar comandos de la consola.
- ***Edit File***. Desde aquí se nos permitirá la edición de los distintos archivos que deseemos utilizar.
- ***Factory***. Sirve para devolver el sistema a su estado primitivo (por defecto)
- ***Halt System.*** Aquí podremos apagar el router desde el host.
- ***Ping.*** Con esto podremos realizar ping
- ***Reboot system.*** Aquí podremos pedir reiniciar el sistema.
- ***Router.*** Aquí podremos ver los datos de la tabla de router.
- ***States.*** Aquí podremos observar las conexiones realizadas
- ***Traceroute***. Con esto podremos realizar traceroute a la dirección que deseemos
- ***Packet Capture***. Aquí podremos realizar una captura de paquetes.

ANEXOS C

INSTRUCTIVO PARA USO DE INTERNET EN LABORATORIO # 2

ANTECEDENTES

Considerando que:

a. Los estudiantes durante las clases tendrán derecho a utilizar el laboratorio de computación asignado con la conexión a Internet para prácticas en las diferentes asignaturas del Bachillerato en Informática especialización Administración de Sistemas o la materia de Computación en el Bachillerato General según cronograma horario establecido al inicio de cada año lectivo.
b. El personal docente y administrativo de la institución podrá hacer uso del laboratorio cuando exista disponibilidad.
c. Los docentes y estudiantes fuera del horario de clases tendrán derecho a utilizar el laboratorio de cómputo que se encuentra disponible con la conexión a Internet, previa presentación de la credencial respectiva y bajo responsabilidad de un docente del área de informática, u otro previo permiso o asignación de autoridad respectiva.
d. Existen sitios o páginas de internet que ofrecen información ofensiva para los estudiantes, misma que puede ser vista sin dificultad y más aún puede ser descargada y dejada a simple viste de otras, así como
e. Sitios o páginas que distraen la atención durante la jornada de práctica en el laboratorio asignada con conexión a internet.

RESUELVE:

Colocar un servidor en el laboratorio # 2, el mismo que:

1. **Facilitará el ingreso a los equipos de laboratorio de computación asignado con conexión a internet a:**

   a. Los estudiantes durante las horas de práctica de las diferentes asignaturas del Bachillerato en Informática especialización Administración de Sistemas o la materia de Computación en Bachillerato General según cronograma horario establecido al inicio de cada año lectivo.

b. Al personal docente y administrativo de la institución podrá hacer uso del laboratorio cuando exista disponibilidad.
c. Los docentes y estudiantes fuera del horario de clases tendrán derecho a utilizar el laboratorio de cómputo que se encuentra disponible con la conexión a Internet, previa presentación de la credencial respectiva y bajo responsabilidad de un docente del área de informática, u otro previo permiso o asignación de autoridad respectiva.

2. Restringir el acceso a la información que solicita el usuario de la siguiente manera:

a. Si el usuario solicita algún tipo de información de una página o sitios de internet que ofrecen información ofensiva para los estudiantes, no será mostrada, se redirige la solicitud a la página de una de los buscadores más utilizados. Ejemplo: www.google.com al usuario le parecerá que no se puede mostrar; de esta manera se le impide mostrar, descargar o que deje a simple viste de otros usuarios.

b. Los Sitios o páginas que se consideren que distraen la atención durante la jornada de práctica en el laboratorio asignada con conexión a internet. Ejemplo redes sociales como www.facebook.com u otra de acuerdo a la disponibilidad de las mismas.

3. Horario de las restricciones:

a. Las restricciones tendrán efecto cuando se encienda el servidor ubicado en el laboratorio # 2.

b. La jornada de trabajo establecida en el plantel es de 7:00 a 15:30 de lunes a viernes.

4. Encendido y pagado del servidor

a. El docente o responsable que tenga asignado la primera hora de práctica el horario establecido para práctica al inicio de cada año lectivo será el encargado de encender el servidor.

b. El docente o responsable que tiene en su horario de práctica la última hora será el encargado de apagar el servidor y verificar que todos los equipos estén apagados para proceder asegurar el mismo.

ANEXOS D

CORTAFUEGOS Y SERVIDORES PROXY PARA DIFERENTES SISTEMAS OPERATIVOS

Cortafuegos	Servidores proxy
Pfsense: es una distribución basada en FreeBSD, para usarlo en servicios de redes LAN y WAN tales como firewall, enrutador, servidor de balanceo de carga, derivada de m0n0wall. Su objetivo es tener un cortafuego (firewall) fácilmente configurable a través de una interface web e instalable en cualquier PC, incluyendo los miniPC de una sola tarjeta. Es una solución muy completa, bajo licencia BSD y, de libre distribución. Otros ejemplos de cortafuegos disponibles basados en **Linux,** FreeBSD o OpenBSD: Firestarter, Zorp GPL, Turtle, LutelWall,	**Proxy con Pfsense:** Su finalidad más habitual es la de servidor proxy, que sirve para interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc. **Squid Proxy Caché Server:** Permite compartir una única conexión a internet, optimiza su conexión ADSL, sin costo de licencias adicionales. Almacena las páginas más vistas para optimizar ancho de banda y acelerar la

Floppyfw, Guarddog, IPCop, Endian, Smoothwall, m0n0wall. En Linux, el cortafuegos por omisión es IPTables **SmoothWall Express:** una distribución de GNU Linux gratuita específica para cortafuegos (firewall) para todos los equipos de la red con un equipo normal. **ZEROSHELL**: Es un Firewall gratuito que tiene las características de los de los equipos complejos de seguridad, es una distribución. Linux para servidores y dispositivos embebidos, que provee de servicios de red. Zeroshell no se integra con Squid, ya que no recoge las páginas Web.	navegación. Realiza un control sobre los sitios que los usuarios visitan, además filtra contenidos indebidos, permitirá sacar todo tipo de estadísticas por usuario, sitios navegados, etc. Frena la navegación a sitios no productivos. Funciona en la mayoría de sistemas operativos disponibles, incluyendo Windows y está disponible bajo la GNU GPL. Los sistemas de Squid] se están ejecutando actualmente en un golpe de tasa de aproximadamente el 75%, cuadruplicando la capacidad de los servidores Apache detrás de ellos. Es muy confiable, robusto y versátil. No es conveniente utilizar un sistema operativo con posibles vulnerabilidades como Servidor Intermediario
Potentes cortafuegos para Windows® que protegen su equipo al evitar que los usuarios no autorizados puedan acceder a su sistema a través de Internet o de otra red.	Bajo el sistema operativo Windows algunos de los Servidores que permiten el acceso a Internet en diferentes ordenadores, con una sola conexión, en red local. Aportan una gran seguridad y limita sitios

Ejemplos: **Para WinXP/Vista/7,** PC Tools Firewall Plus, ZoneAlarm Pro, Sunbelt Kerio Personal Firewall, McAfee Personal Firewall Plus, Sygate Personal Firewall. En idioma español y otros. **Sistema operativo: Win2k/XP/2003/Vista:** Agnitum Outpost Firewall Pro, **Toda clase de sistemas operativos a parte de Windows Linux, Mac, etc.:** Kerio WinRoute Firewall, Licencia Gratis: Comodo Firewall Pro.	Webs. Tienen integrados: Anti-Spyware, Anti-Phishing, Antivirus, Antispam, Firewall y filtros para webs. Algunos ejemplos para diferentes tipos de licencia. **Licencia Shareware:** All Aboard! SE 2.5, All Aboard! SE 2.5, AllegroSurf 7.0.0.2, Avirt Soho 4.3, PPPshar Pro 1.9, GProxy 1.26, RideWay 2.40**.** **Licencia Libre:** FreeProxy 3.81, ChProxy 2.0, AnalogX Proxy 4.14, Intergate 9.02, Proxy+ 3.00. **Demo:** ProxyMail 4.3.2

Ejemplos de cortafuegos y Servidores Proxy

BIBLIOGRAFIA

1.- BARRIOS DUENAS, J. Implementación de Servidores con GNU/Linux. Sicilia. México D.F. 2009. 614p.

2.- CASTRILLON, W.A. Implementación de Proxy con Pfense. CENTRO DE SERVICIOS Y GESTION EMPRESARIA. Medellín-Colombia. Sena. 2011. 26p.

3.- GONZÁLEZ VALENZUELA, F. et al. PC- Router. Proyecto redes de computadoras. Universidad Técnica Federico Santa María UTFSM. DEPARTAMENTO DE ELECTRÓNICA. Valparaíso-Chile. s.e. 2008. 11p.

4.- SÁNCHEZ ALLENDE, J. y LÓPEZ LÉRIDA, J. Redes. s. L. McGraw – Hill. 2008. p.12.

5.- TANENBAUM, A.S. Redes de computadoras. 4ta.ed. México. 2003. Pretince Hall. pp 15-64.

6.- AVILÉS CHACÓN, H.D. Desarrollo de una guía para el control de brechas de seguridad en servicios de internet y aplicada a PETROPRODUCCION. Facultad de Informática y Electrónica. Ing. Sistemas Informáticos. Escuela Superior Politécnica de Chimborazo. Riobamba - Ecuador. Tesis 2009. 178p.

7.- MOYANO YEROVI, C.F y VILLA YÁNEZ, V. A. Análisis de seguridad de los protocolos de internet Tcp/Ip y su prevención, aplicado a los servidores de la ACADEMIA CISCO. Facultad de Informática y Electrónica. Ing. Sistemas Informáticos. Escuela Superior Politécnica de Chimborazo. Riobamba - Ecuador. Tesis 2010. pp. 196-201.

8.- SOLANO JIMENEZ, J. M Y OÑA GARCÉS, M. B. Estudio de portales cautivos de gestión de acceso inalámbrico a internet de la ESPOCH. Facultad de Informática y Electrónica. Ing. Sistemas Informáticos. Escuela Superior Politécnica de Chimborazo. Riobamba – Ecuador. Tesis 2009. 164p.

9.- INSTALACIÓN DE PFSENSE

- http://www.albertograjeda.com/2010/02/guia-rapida-instalacion-pfsense.html. 2011/03/25
- http://www.taringa.net/posts/linux/6555753/Tutorial-PfSense_--Instalacion.html. 2011/03/25

- http://www.taringa.net/posts/linux/10422905/Tutorial-instalacion-Squid-Pfsense-2.0-RC-1.0.html
  2011/06/23
  www.scribd.com/.../Manual-de-Usuario-de-Pfsense-Firewall.
  2011/06/23
- http://www.taringa.net/posts/linux/11256800/Tutorial-instalacion-SquidGuard-PfSense-2_0-RC-1_0_.html-
  2011/06/23
- http://doc.pfsense.org/index.php/2.0_New_Features_and_Changes 2011/06/23
- http://translate.google.com.ec/translate?hl=es&langpair=en%7Ces&u=http://doc.pfsense.org/index.php/Installing_pfSense
  2010/05/18
- http://translate.google.com.ec/translate?hl=es&langpair=en%7Ces&u=http://www.iceflatline.com/2010/08/install-and-configure-pfsense-in-your-home-network/.
  2011/03/29
- http://www.javcasta.com/2011/06/18/freebsd-firewall-portal-cautivo-con-pfsense/.
  2011/06/23
- http://www.taringa.net/posts/linux/6246073/5-Distribuciones-Linux-_-1-BSD-para-descargar_.html
  2009/12/06
- http://ricondefreebsd.blogspot.com/2007/04/pfsensebridge-y-no-morir-en-el-intento.html.
  2009/12/06
- http://www.openbsd.org/.
  2009/12/06

10.- FIREWALLS O CORTAFUEGOS

- www. alegsa.com.ar/Dic/Firewalls.php.
  2008/06/18
- http://wared-red.blogspot.com/2011/07/firewall-pfsense.html
  2008/06/18
- http://es.wikipedia.org/wiki/Cortafuegos.
  2010/06/18
- http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29
  2008/06/18
- http://www.linuxparalapyme.com/os_firewall.php.
  2008/07/22
- http://www.monografias.com/trabajos11/linux/linux.shtml-
  2008/07/22
- http://www.infospyware.com/Firewall/Comparar%20cortafuegos.htm
  20008/07/22
- http://www.eumed.net/cursecon/ecoinet/seguridad/cortafuegos.htm 2008/07/22
- http://www.elprisma.com/apuntes/ingenieria_de_sistemas/cortafuegos/.
  2009/08/26
- http://www.jbex.net/que-es-un-firewallcortafuegos.html/.
  2009/08/26
- Video tutoriales para configurar cortafuegos de los sistemas operativos.
  2009/08/26
- http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)/.
  2009/08/26
- http://www.unixmexico.org/.
  2009/08/26

11.- REDES DE COMPUTADORAS

- http://empresas.telefonica.es/asp/catalogo_servicios/comunicaciones_privadas/datos/teletrabajo/acceso.htm/.

2009/12/06

12.- SERVIDORES

- http://html.rincondelvago.com/cortafuegos-y-servidores-proxy-bajo-linux.html/.

  2009/12/06

- http://www.linuxparatodos.net/portal/staticpages/index.php?page=servidor-proxy&mode=print/.

  2009/12/06

- http://www.alcancelibre.org/staticpages/index.php/donativos/.

  2009/12/06

- http://www.alcancelibre.org/forum/.

  2009/12/06

- http://www.janaserver.de/.

  2009/05/21

- http://www.proxycollection.com/.

  2009/05/21

13.- SEGURIDAD EN INTERNET

- www.adrformacion.com/cursos/seguint/seguint.html/.

  2009/08/26

- http://observatorio.cnice.mec.es/modules.php?op=modload&name=News&file=index&catid=&topic=24/2009/02.

  2009/08/26

- http://www.adrformacion.com/cursos/seguint/leccion3/tutorial2.html/.
  2009/08/26
- www.DesarrolloWeb/manuales/ayudas-tecnicas/seguridad-en-la-red 2009/03/27
- www.DesarrolloWeb/manuales/ayudas-tecnicas/estrategias-de-seguridad-inormaticaseguridad-en-la-red/.
  2009/03/27
- http://seguridadyredes.nireblog.com/post/2007/12/28/sistemas-de-deteccion-de-intrusos-y-snort-i.
  2009/03/27
- http://alertaenlinea.gov/inalambrico.html/2008/05.
  2009/03/27
- http://brsi.blogspot.com/2006/12/host-intrusion-prevention-system-este.html/.
- 2009/02/23
- http://es.wikipedia.org/wiki/Lista_de_control_de_acceso.
  2009/02/23

14.- SQUID

- http://www.linuxparatodos.net/portal/staticpages/index.php?page=19-0-como-squid-general/.
  2008/06/18
- www.squid-cache.org/
  2008/06/18.